temtum

Cryptocurrency. **Evolved.**

temtum™ & The Temporal Blockchain

Cryptocurrency crosses into the mainstream

Contributors:

Founders: Richard Dennis, Dr Gareth Owenson

Cryptocurrency. Evolved.

Abstract

temtum has set out to solve all inherent problems faced by not only many existing cryptocurrencies but peer-to-peer blockchain networks as a whole both now, and in the most technologically advanced of futures, where speed, scalability, security and high resource requirements are most pertinent and continue to limit adoption. The Temporal Blockchain, developed by Dragon Infosec, combined with temtum's innovative Consensus Algorithms and AI powered Performance Integrity Protocol, removes network competition, drastically improves network efficiency and uses a source of light for quantum effect randomness. The result is a fast, quantum secure, environmentally friendly and highly scalable payment coin that has been developed to both integrate into existing payment infrastructures and deliver as a standalone cryptocurrency, allowing even the most under resourced individuals to benefit from immediate, feeless transactions, no matter who or where they are in the world - TEM.

Our Vision.

We believe in the power of blockchain.

It provides amazing opportunities that have so far barely been touched on. For cryptocurrencies to thrive, blockchain now needs to take the next step in its evolution.

And that’s where temtum comes in. temtum can help to secure a truly distributed, decentralised and democratic future for financial transactions.

It is a future that does not destroy the environment. A future for everyone, wherever they live in the world, in which the benefits of cryptocurrencies are available and accessible forall.

We have not only seen this positive future, we have designed the technology, built it, tested it and mapped out how it will be implemented as the most effective medium of exchange.

Welcome to the future of finance. **Welcome to temtum.**

Contents

temtum

Cryptocurrency. Evolved.

ABSTRACT 2

OUR VISION 3

EXECUTIVE SUMMARY 9

- » temtum's story 11
- » Dragon Infosec commercial objectives & temtum 11
- » A world-class team 11

TEMPORAL – A STEP-CHANGE FOR BLOCKCHAIN 12

- » The problems with current blockchain technology 13
- » How temtum solves these problems 14
- » A step-change in the evolution of blockchain 14

THE TECHNOLOGY 16

Introduction 17

1) The key technology features 18

- » The temtum Consensus Algorithm and Temporal Blockchain 18
- » Temporal scalability 18
- » True decentralization for low-power devices 18
- » How Temporal works 19
- » No hardcoded block size limits 20
- » Temporal block structure 20
- » Random numbers 20

2) The temtum Consensus Algorithm 22

- » How the Consensus Algorithm works 24
- » NPD Process 25
- » A democratic transaction protocol 25
- » Removing the possibility of forks 25
- » Node descriptor format 26
- » General block validation 27

3) The Optimized Routing Algorithm 27

4) Random number generation and the NIST Beacon 28

- » How the NIST Randomness Beacon works 29
- » NIST Randomness Beacon security 30
- » Implementing NIST 31
- » temtum NIST Integration 32
- » The probabilities of determining NIST Values 32

Overall temtum network architecture 35

Resilience to attack 37

REAL-WORLD APPLICATIONS 39

temtum as a medium-of-exchange cryptocurrency 39
» TEM currency features 39

Vision for temtum as a mobile POS payment system 41
» Integration into existing payment models 41
» Benefits 42

TEM Mobile PoS payment solution 42
» Partnering with banks and/or payment cards 43

Online gaming 44
» Fiat on-ramp 45

e-Commerce payment gateway 46
» The e-commerce market 46
» The returns dilemma 46
» temtum as a payment gateway 46
» The buying process 47

COMPETITOR ANALYSIS 48

Introduction 49
» Bitcoin 49
» Nano 52
» Hedera 52
» Ripple 53
» Stellar 54

NETWORK INTEGRATION 55

Introduction 56

Deployed network and applications 56

temtum API 57

Wallet system 60

temtum keyboard 60

SMS payment transfers 61

Network performance 62

- » Transactions per second (TPS) 62
- » An energy-efficient network 63
- » Transaction costs 64

CREST-approved security testing 65

TECHNOLOGY ROADMAP 68

Application and functionality development 69

IoT and mobility implementations 69

- » Phase 1: BMW i8 69
- » Phase 2: Car-to-car 69
- » Use case - In-car wallet 70
- » Fitbit Ionic 70
- » DJI spark 70

Homomorphic Encryption 70

- » Homomorphic encryption and anonymity of votes 70
- » What is homomorphic encryption? 70

Existing payment system integration 71

- » Private fiat bank context 72

temtum national bank credit and debit card system 72

Network technology 73

Increased sources of randomness 73

Smart contract platform 73

Leader Selection Algorithm 75

- » Phase 1: Performance Integrity Protocol 77
- » Phase 2: Leader Selection 79
- » Phase 3: Block confirmation 80

Double blockchain 81

Intrusion Detection Algorithm 81

Sharding and delegation 81

Process for ISO 27001 accreditation (information security) 82

CONCLUSION 83

THE TEAM 85

- » Board of Directors 87
- » Developers 88
- » Advisory Board 89
- » temtum advisors 90
- » Partners 91
- » Pen testing andthird-party security 92

TERMS AND CONDITIONS 93

GLOSSARY OF TERMS 95

Executive Summary

temtum

Cryptocurrency. Evolved.

A new cryptocurrency called temtum will be the most technologically advanced and globally preferred blockchain coin (TEM) and will set new standards in security, speed, resource requirements and scalability. temtum's vision is to become the most widely used cryptocurrency in the world, adopted into mainstream payment markets by regular consumers and citizens on every continent.

The name 'temtum' represents a combination of two of the main concepts that underpin this technology:

- The Temporal blockchain ('tem') and quantum randomness ('tum'). We will explain these concepts in detail within this paper, particularly in the 'Technology' & 'Network Integration' sections.

There are a lot of cryptocurrencies now in existence, but critically none has yet succeeded as a mainstream form of payment used by millions of regular people around the world for everyday transactions.

temtum changes all of that and represents a step change in the evolution of cryptocurrencies. It is also far more than just theory; it is a completed network that is ready for mainnet deployment.

temtum is an efficient, quantum-secure, ultra-fast, non-resource intensive and environmentally friendly payment coin (using the acronym 'TEM'), and an alternative to traditional fiat money (government-printed currency). It can be used on a standalone basis wallet-to-wallet, and can also be integrated into payment systems worldwide, serving as a payment platform for both consumers and businesses.

temtum's ambition is to be much more than a cryptocurrency that merely benefits speculators and which is only meaningfully used by tech-focused blockchain communities – it has an underlying purpose enabled by the most sophisticated and robust blockchain technology on the market: Temporal Blockchain developed and licensed by Dragon Infosec. temtum builds on the significant opportunities of blockchain technology and overcomes many of the existing limitations faced by current peer-to-peer networks, which means that they have only been adopted in a limited way.

As such, temtum offers a giant leap forward with technology that has the potential to meaningfully transform the way that value is globally exchanged and stored. Perhaps the greatest leap forward of all is that it can be run on almost any device connected to the internet – including smartphones and IoT devices, cars and drones. Our integration of the temtum network in a BMW i8 is a world-first in terms of using a car as a full node in a network, without the need for additional hardware. This makes it accessible to ordinary people who have so far largely been excluded from the benefits of blockchain technology.

temtum has established technical leadership and a dedicated team of developers who will continue to extend intellectual property development by executing our intended technical and integration roadmap described elsewhere in this document. Included in these innovations are sharding and delegation, fiat money integration via existing banking infrastructures and smart contract capabilities.

Point-of-sale (POS) and mobile payment solutions have been developed, with the technical framework described in detail in this paper, and are ready to deploy once banking and payment providers are secured aspartners.

The integration of temtum into gaming, Esports and e-commerce sites has been demonstrated through the development of demo platforms and plugins, which can enable fast implementation with partners as part of our intended roadmap.

temtum's story

temtum was founded by Dragon Infosec CTO Richard Dennis, working with his global team of cybersecurity and cryptography experts, Dr Gareth Owenson and Cintya Aguirre. Together they set out to resolve issues inherent in peer-to-peer networks, starting with Tor and Open Bazaar, and finally Bitcoin, before developing a new technology that can be used by and integrated with mainstream payment networks for and by ordinary people.

Richard took theoretical mathematics and academic research and developed it into a blockchain technology known as Temporal, owned by Dragon Infosec and perpetually licensed to temtum. Temporal has been independently tested (BSI) and deployed into a live working network, providing the foundations for a fast, secure, highly scalable and environmentally conscious payment coin – temtum.

Dragon Infosec commercial objectives & temtum

Dragon is in advanced discussions and has received letters of intent to implement sovereign digital currencies, based on its Temporal blockchain technology, in a number of states in Africa. It is expected that all licence fees and any other revenues due to Dragon under such agreements will be transacted only in temtum thus increasing the transaction volume of TEM. Other products or business avenues developed by Dragon will also require payments to be completed in TEM.

Temporal technology represents a paradigm shift from current blockchain networks as an evolutionary step for the next-generation of technology in the industry – and also offers significant advantages compared to other non-blockchain cryptocurrencies. temtum's proprietary Consensus Algorithms are truly new and inventive solutions to the industry's most pressing pain points.

A world-class team

temtum founder and senior cryptography advisor Richard Dennis and CISO Dr Gareth Owenson. They are joined by Director David Shimmon and the best brains in cryptography and blockchain, alongside a senior team rich in banking infrastructure, commercial acumen and financial services experience.

The team has global coverage, with team members based in the British Virgin Islands, the Cayman Islands, San Francisco, London, Hong Kong, Frankfurt, Ecuador and Belarus.

Find the full team profiles feature in 'The Team' section of this paper.

Temporal - A step change for blockchain

temtum

Cryptocurrency. Evolved.

Temporal Blockchain technology transforms the way the blockchain works by reconstructing how peer-to-peer networks scale. It operates with less power, energy and storage, and processes transactions on very low-resourced devices at extremely high speeds, with an unparalleled degree of security. The temtum network can be scaled rapidly and at minimal cost. temtum eliminates the need for centralized pools of specialized hardware, delivering a blockchain network that's environmentally conscious and can be run on any device connected to the web – even a smartphone.

This means that our vision of a truly decentralised, fully scalable network that can be placed in the hands of the many rather than the few is fully achievable. Yet with previous blockchain technology – which theoretically supported a similar vision – that simply wasn't the case. Our technology innovations have supported the necessary evolution of blockchain, which in turn means that the temtum cryptocurrency represents a compelling mass-market proposition at a global level.

The problems with current blockchain technology

Blockchain is still an emerging technology. It has already started to transform a wide range of industries around the world by providing a digitized, immutable and secure network for transacting, sharing and distributing data without a central authority. This provides a number of significant theoretical benefits when compared with existing technologies and methods, such as improved transparency, traceability and security, as well as increased efficiency and speed of transactions. Most importantly, financial transactions are no longer reliant on trust – they are cryptographically proven.

And yet blockchain networks that have already been deployed have suffered from a number of downsides and concerns that have meant that they have failed to deliver on their promise and are yet to see significant adoption. Chief among these downsides are:

Scalability:
Current blockchain technologies are not truly scalable. They are not able to be fully decentralised and in many cases require high entry points to participate in them e.g. massive computational power.

Speed:
Many blockchain technologies, including Bitcoin, are enormously slow. Bitcoin can take 10–15 minutes per transaction which makes it thoroughly unsuitable as a mainstream form of payment. The majority of alternative high transaction technologies are not blockchains.

Resource intensity:
Many leading cryptocurrencies use highly wasteful and restrictive consensus mechanisms such as proof-of-work, which require enormous energy use and have a significant environmental impact.

Security:
Blockchain based cryptocurrencies' pseudo-random generation of keys is open to exploitation by sophisticated hackers, with quantum computing increasing the likelihood of predicting software-generated values.

How temtum solves these problems

The fact that current blockchain networks have limitations at their core, means that they cannot satisfy the key transaction demands for many of the industries and applications which should have the highest need for blockchain networks, such as large global payment networks and credit card companies. This is how temtum addresses each of these flaws in current blockchain networks:

Scalability: The Temporal Blockchain eliminates the need to store the entire chain history on all nodes by locally archiving data, while preventing competition in node selection. This significantly reduces resource requirements and allows anyone with a basic form of technology – such as a smartphone user – to fully participate in the network, delivering true decentralization and infinite scalability.

Speed: The speed of the temtum network is limited only by the hardware and bandwidth of network participants. We have created a highly efficient Consensus Algorithm and removed block size limitations in order to confirm transactions into a block extremely quickly, with a maximum confirmation time of 12 seconds. Once included in a block, a transaction is confirmed – there is no need to wait for additional blocks to be added subsequent to the initial block, as is the case with Bitcoin, due to the impossibility of a malicious fork.

Resources: temtum's Consensus Algorithm, constructed around leader nodes and our innovative Node Participation Document, removes the need for mining and wasteful, inefficient and restrictive Consensus mechanisms such as proof-of-work. temtum uses substantially less energy and has less environmental impact compared to POW networks. We estimate that the Bitcoin network is 16,573,693 times more expensive than the temtum network based on energy costs alone, assuming both networks are operating at the same size. The Bitcoin network is currently limited to a maximum transaction throughput of seven transactions per second. The average fee for a Bitcoin transaction from 2017-2018 was $57.35 – and the total cost of a Bitcoin transaction in the same time period, including miner and energy fees, was $104.70[1].

Security: Temporal is a quantum-secure blockchain network that uses a photon source for genuine random number generation alongside next-generation hashing algorithms. These prevent the network from being vulnerable to theoretical attacks – even in the case that quantum attacks become commonplace in the near future.

A step-change in the evolution of blockchain

Perhaps the key invention in the original Bitcoin white paper (2008) was the integration of the proof-of-work consensus mechanism. This allows all nodes that comprise the Bitcoin network to ensure they share the same copy of the distributed ledger so that it is impossible to double-spend. The proof-of-work mechanism is essentially a method of randomly selecting the next node that will confirm previous transactions in a way that prevents the reasonable economic prediction of the next confirming node.

Proof-of-work is effective at a certain scale, but it is also extremely resource and energy-intensive, and has failed to adapt to growth, as convincingly argued in a 2019 working paper by the Bank for International Settlements (BIS). [2] This paper states that proof-of-work can only achieve payment security if mining income is high, but if that is the case, the transaction market cannot generate an adequate level of income. As a result, liquidity is set to deteriorate substantially in years to come. This is just one of the reasons why for blockchain cryptocurrencies to be truly effective, there needs to be a step-change in their evolution. And that is precisely what we believe temtum delivers.

The temtum Consensus Algorithm, by contrast with Bitcoin, is highly secure and does not require intensive computational resources. It also eliminates block size limitations and implements

[1] https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

'Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies', January 2019:

[2] https://www.bis.org/publ/work765.htm

improved network routing, which means that the temtum network can handle increasing loads as required, which solves the scalability problem. The only limitations governing the number of transactions per second that temtum delivers are hardware and network bandwidth.

The temtum network incorporates – and is enhanced by – the Temporal Blockchain, a new mechanism that allows local nodes to define themselves as 'Temporal nodes' to archive data in order to minimize storage space usage. This follows the same logic as Bitcoin in terms of establishing a timestamp network, but crucially it does not require proof-of-work mining. Instead, although data is archived locally, the Temporal system has been designed to ensure the integrity of the blockchain – making it possible for nodes to validate previous transactions without downloading and storing the entire blockchain.

This data storage method allows low-power devices to fully participate in the temtum network and confirm transactions without requiring the resources demanded by traditional proof-of-work blockchain networks such as Bitcoin. The combination of the temtum Consensus Algorithm and Temporal technology allows the temtum network to deliver extremely high transaction throughput and short transaction confirmation times with low resource requirements.

We have used laboratory tests followed by a live deployment over globally distributed servers to confirm a throughput of up to 120,000 transactions per second (a multiple of the peak capacity of 56,000 TPS on the VISA system).[3]

The technology behind temtum is already fully developed, including mobile and web applications, which are described throughout this document. The temtum live mainnet will be deployed at the same time as coin distribution is carried out. temtum coin (TEM) will be delivered as a fully operational form of payment on day one of genesis block (the first block of any blockchain).

[3] https://usa.visa.com/about-visa/visanet.html

Technology

temtum

Cryptocurrency. Evolved.

Introduction

This section provides an overview of the groundbreaking new technology behind temtum. Please refer to the glossary at the end of this white paper for a list of definitions.

The temtum network achieves truly decentralised scalability, near instant transaction speeds and unprecedented transaction throughput, using low resources and future-proof cryptographic security.

With our improved network routing, the removal of the block size limit and a system architecture that ensures a single, randomly selected node confirms all transactions for 60 seconds, the only limitation to transaction throughput is the hardware and bandwidth of network participants. This is shown by the fact that we have demonstrated simulated transaction throughput speeds of 120,000 transactions per second in a laboratory environment.

The critical elements of the temtum network architecture are the Temporal Blockchain, the Consensus and Routing Algorithms, and the use of proven truly random numbers based on quantum interference science.

- Temporal technology provides the temtum network with an archivable blockchain, distributing blockchain data storage across a range of specialized nodes in order to allow low-powered devices to participate in the temtum network.

- temtum's **Consensus Algorithm** is a unique approach to blockchain consensus, which by definition allows one – and only one – leader to be selected at any given time. This eliminates any potential malicious fork. It also eliminates the energycost associated with proof-of-work consensus model, improving the overall network efficiency.

- The **Routing Algorithm** removes the need for the use of any type of gossip protocol because, by design, each node has an accurate and up-to-date global overview of the network and transactions are sent only to the leader node, rather than to all nodes.

- The **NIST Randomness Beacon** uses quantum mechanical effects to generate proven truly random numbers that are used to secure the Temporal Blockchain network. Other equivalent sources of randomness have been identified andproven and are described in the roadmap section of this document as alternatives.

1) The key technology features

The key technology features were designed and coded to be a state-of-the-art payment coin.

The temtum Consensus Algorithm and Temporal Blockchain

As mentioned above, Temporal allows local nodes to define themselves as 'Temporal nodes' and to archive data, which minimizes storage space use. The Temporal system ensures the integrity of the blockchain – even though data is archived locally, it is possible for nodes to validate previous transactions without downloading and storing the entire blockchain.

Archive nodes operate as a subset of a Temporal node and perform Temporal node functions as well as archiving the entire history of the Temporal Blockchain. The increased resource commitment required to operate an archive node results in a smaller distribution of archive nodes compared to ordinary nodes, much like master nodes on other networks. Our simulation data predicts low archive node participation frequency within the first year of launch as we would expect. Any node participating in the temtum network can also operate as an archive node: if the node has the required storage space it can act as an archive node.

Temporal scalability

Temporal allows for short-term data storage on nodes, while maintaining the integrity and full history of the blockchain.

This data storage method allows low-power devices to fully participate in the temtum network and confirm transactions without requiring the resources demanded by traditional proof-of-work blockchain networks such as Bitcoin. The combination of the temtum Consensus Algorithm and Temporal technology allows the temtum network to deliver extremely high transaction throughput and short transaction confirmation times with low-resource requirements.

We want all users to be able to fully participate in the temtum network, regardless of the resources they are able to contribute. The temtum network has been designed from the ground up to run at full capacity on low-powered devices such as smartphones or IoT devices. The only prerequisite to network participation access to an active internet connection.

True decentralization for low-power devices

The prototype temtum network has been proven to be fully deployed and functional on a wide range of devices that include low-power personal computers, servers, basic Android mobile devices, and even a smart car – a BMW i8. We have demonstrated that the prototype network can operate at high speeds despite the varying computational and storage capacity of the resources available to it – and deliver higher transaction throughput while using less computational power and energy than alternative proof-of-work blockchain networks such as Bitcoin.

Temporal nodes can check the hash of the block to ensure it matches the hash stored in their blockchain in order to ensure archive nodes provide accurate block data when queried. Nodes do not retain the full blockchain but do retain all blockchain headers from genesis. This data set, while small, provides security against the possibility of malicious block injection. Nodes are also able to check the NIST Randomness Beacon timestamp (described later in this document) that the block was mined with, and will do so in order to determine authenticity.

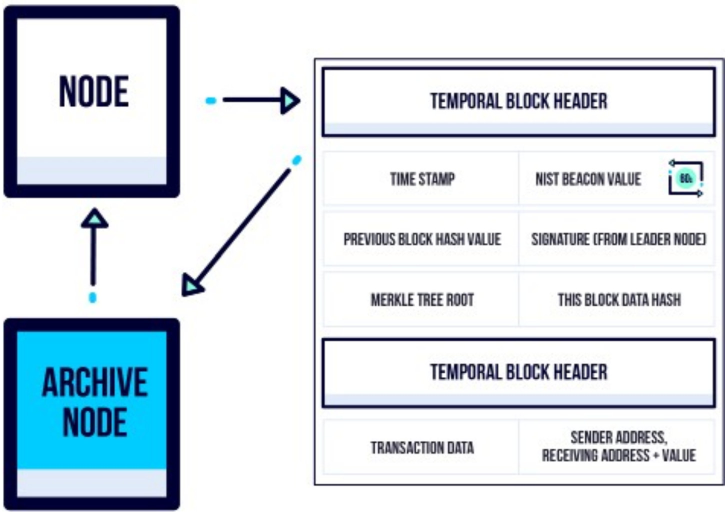


Fig 1: Hash check

How Temporal works

Temporal nodes store the blockchain as defined by the node administrator, which can range from thirty days to every block from genesis. Nodes are responsible for confirming all transactions. During our research, we concluded that the majority of transactions within major cryptocurrency blockchains use UTXOs from the previous 30 days. Our simulations demonstrate that only 2% of all transactions require data for a transaction older than 30 days. Should this data be required, however, it's still available – it is not deleted from the network.

Archive nodes participate in the temtum network as Temporal nodes. They function as block leaders and confirm transactions when selected. As well as working as Temporal nodes, Archive nodes store all blockchain data and provide UXTOs for any given user when queried by another node. This allows confirming nodes to ensure that a user possesses a sufficient balance to fund a transaction.

The properties of the blockchain ensure that potentially malicious archive nodes are not able to forge artificial transactions into previous blocks as an artificial transaction hash would not match to the Merkle tree maintained by the querying node and thus be detected as fraudulent.

Temporal's reduction in storage space requirements allows network participants to cap hard drive demand. The storage space requirement associated with temtum network participation can be capped to customizable levels, such as 3GB over a 30-day period – a dramatic reduction from the 205GB[4] currently required of Bitcoin nodes.

Temporal reduces more than just storage requirements to deliver unprecedented scalability. Our unique Consensus Algorithm reduces network traffic by a factor of over 7,000 on a 10,000 node network, while the lack of proof-of-work minimizes energy and computational requirements for all nodes. The elimination of gossip protocol redundancy establishes an ecosystem in which a single node confirms all transactions – with the same network size as Bitcoin, the temtum network saves 9,950 machines from needlessly completing expensive computational work.

[4] https://www.blockchain.com/en/charts/blocks-size as at 25th Feb 2019.

No hardcoded block size limits

Most contemporary blockchain networks enforce a hardcoded block size limit that restricts the number of transactions that can be included in a block in order to reduce blockchain growth and artificially limit network scale. Even if this limit was reduced, however, any given blockchain would still grow at a rate that would preclude average home and mobile users from participating in the network.

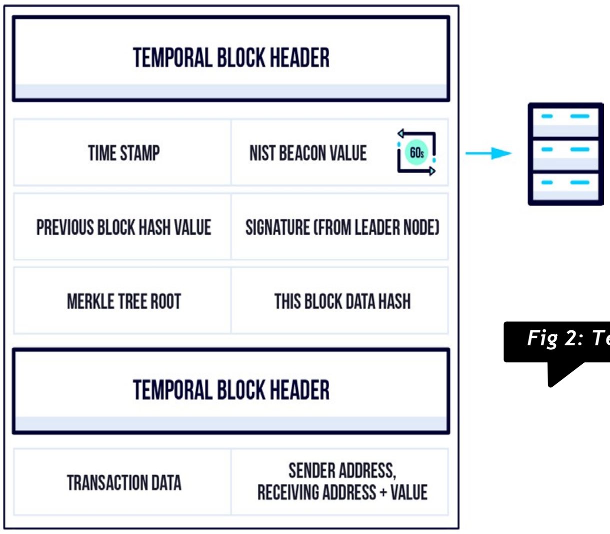


Fig 2: Temporal Block

The concept of hardcoded block size restrictions stands against the original Bitcoin vision of Satoshi Nakamoto and are a direct cause of hash power centralization within the Bitcoin ecosystem, in which three VPS hosting providers host 72% of all full nodes on Bitcoin.

Temporal has no such block size limit in place, and this means that there is no theoretical limit on how many transactions can be included in a block. Bitcoin, for example, generates one block every 10 minutes. Through extensive research, we have determined that the optimum block generation speed is 12 seconds per block. A single leader within the temtum ecosystem will be responsible for five blocks, each of which are cryptographically linked to other blocks.

Temporal block structure

The block structure of our network separates block headers from block data. The block data is stored in a Merkle tree structure – but Temporal technology makes is possible for nodes to retain only block header information, which includes NIST Randomness Beacon timestamp data, the signature of the node responsible for block creation, the hash of the data and the Merkle tree.

The key innovation in the Temporal block structure is that it is not possible for malicious actors to retroactively recreate a valid block and present it as a genuine block, even if the node validating the transaction has deleted the body of the block data from the blockchain they store.

Random numbers

The NIST Randomness Beacon, which is described in detail below, publishes a new certifiably random number every minute. This data is also archived by NIST and can be validated easily by sending a query, containing the timestamp of the period for which you wish to receive the beacon value, to NIST.

The same NIST Randomness Beacon value used to select the next leader node is also inserted into the block. This improves efficiency by removing the need to query two sources for randomness and leverages the highly secure nature of the NIST Randomness Beacon – there are no security issues associated with using the same value for different roles twice in one 60-second time frame.

The Node Participation Document (NPD) is similarly archived by authority nodes – any node is able to query an authority node to receive the valid NPD for any given timestamp. This system makes it trivial for any network participant to determine which node was responsible for generating any block at any time.

The hashes of all future blocks link back to the hash of the previous block. And this means that, even if a malicious node did somehow obtain the private key of the previously confirming node and generate a legitimate block with the correct NIST beacon signature, the hashes will not match and the network will be able to detect that the block is not genuine.

Should a single bit of data within a block change, a minimum of 50% of the values in the hash must change. The statistical probability of two separate pieces of data possessing the same hash is extremely low.

Our hashing algorithm is built to offer $2^{n^{22^{n^{2}}}}$ collision resistance and 2^n preimage resistance. The probability of a collision attack occurring in our algorithm is represented by the following approximation:

$$p \approx 1 - \exp(-\frac{\frac{1}{2}n(n-1)}{2^{256}}) \approx 1 - \exp\left(-\frac{n^2}{2 \cdot 2^{256}}\right) \approx 1 - \exp\left(-\tfrac{1}{2}\left(\frac{n}{2^{128}}\right)^2\right)$$

If $n \ll 2^{256/2}$ and thus $p \ll 1$ you can use the approximation $\exp(x) \approx 1 + x$ and obtain:

$$p \approx \tfrac{1}{2}\left(\frac{n}{2^{128}}\right)^2$$

Fig 3: Hashing Algorithm

The probability of a collision attack is negligible given that we have significantly less than 2^{128} values. This is the case for any realistic amount of data – an unbroken 256-bit hash is sufficient, but we use a 512-bit hash for all data. The probability that an attacker could generate a block with different contents and a valid hash is unrealistically low. Our block structure is designed specifically to allow Temporal to delete transaction data and this ensures that even if a node becomes compromised in future it cannot be used to edit past blocks.

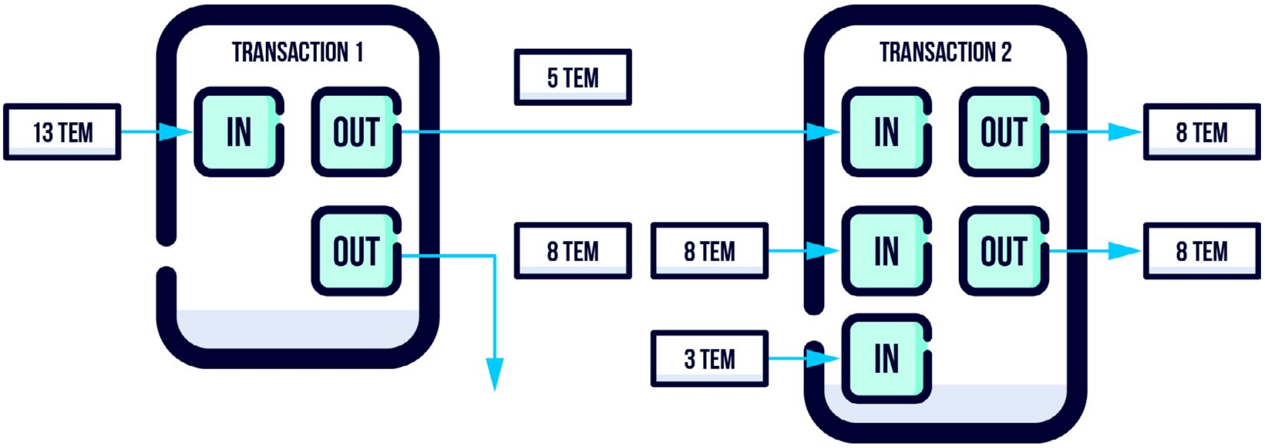
Transactions in the temtum network take place in a similar way to transactions in the Bitcoin network. Transactions reference temtum in the inputs and reassign this value to recipients in outputs. When a transaction is accepted on the network, the pieces of temtum referenced in the inputs are spent and new 'unspent transaction outputs' (UTXO) are created according to the transaction's outputs.

UTXO are used by network participants to track balances. UTXO are created whenever a transaction defines a recipient, and not only when there is a change. UTXO are spent whenever they are used as a transaction input. Each transaction remains an immutable part of the blockchain and can be validated by any network participant at any time.

Therefore, after a UTXO is spent, it is still a transaction output (TXO) – but no longer a UTXO.

For example:

Fig 4: Example UTXO graphic



When a transaction is created, it spends the two UXTO referenced in the inputs. When the transaction is confirmed, every network participant subsequently removes them from their UXTO databases. References in the form of the outputs of the transactions that created the UXTOs remain on the blockchain.

The transaction also creates two new UXTOs – ‘Recipient Output’ and ‘Change Output’. All network participants add these UXTOs to their database. Should a sender spend the capital in the change output rapidly and remove the change output from the UXTO database while the recipient TXO remains unspent, the transaction would be counted in 'Total Transactions with Unspent Outputs.' This is true for any transaction where at least one of the two outputs remain unspent.

The Temporal algorithm deletes all block data from a node's defined point in time. This data does not include the block headers since this contains the NIST beacon data and other important data to secure the structure of the blockchain. If a node was sent a transaction which required past deleted data, then the node would be able to either request this data from an archive node or ask an archive node if the transaction is valid.

This allows Temporal nodes to store a finite amount of the blockchain.

In addition, Temporal nodes can also search the blockchain from the Temporal date to current, and remove any spent transactional information in their databases, further reducing the local storage requirements on the Temporal nodes.

2) The temtum Consensus Algorithm

The temtum Consensus Algorithm ensures that there can only be one possible leader node at any given time. Leader nodes are responsible for all blocks within the 60-second window in which they are block leader, eliminating the potential of a fork. If the leader node goes offline during the time in which it is responsible for block confirmation, all unconfirmed transactions will be rolled into the next leader node’s block. This is entirely different from – and far superior to – current methods of selecting leader nodes, for example proof-of-work and proof-of stake.

In practice, the process works like this:

1. A node is selected to be a leader for 60 seconds.
2. The Node Participation Document NPD is searched, finding the NIST Beacon hash and taking away the public key of each node – the node which is the closest to zero is the next leader.
3. All nodes locally search the NPD and come to the same conclusion on the next leader node.
4. All nodes then forward their transactions to this selected leader.
5. The leader node confirms the transaction is valid – if so, it is added to the block, or else it is dropped.
6. This is done for five blocks; each block is created every 12 seconds.
7. Each block is published to the network and is appended locally to their blockchains.

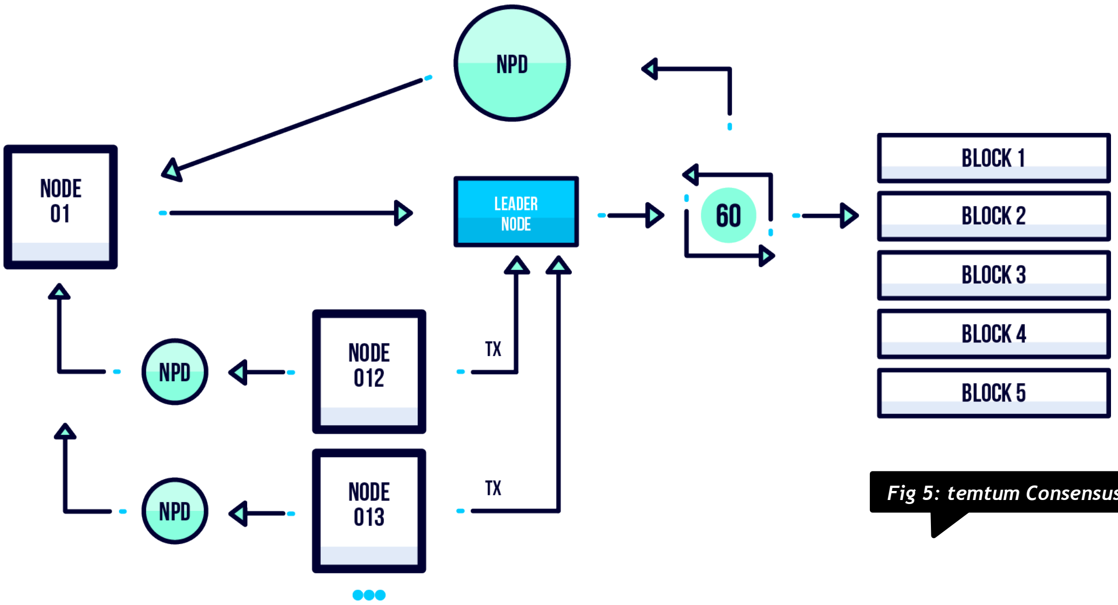


Fig 5: temtum Consensus Algorithm

Consensus is integral to the operation of any blockchain network. The majority of contemporary blockchain networks use resource-intensive proof-of-work algorithms to confirm past transactions. Proof-of-work algorithms serve a role as an economic disincentive to malicious network participation, ensuring that each individual node participating in the network must expend a large amount of energy by performing resource-intensive calculations to identify the confirming node.

In our network, the leader is chosen by a very simple computation which compares the value of the NIST Beacon with the public key of the node. It means that very little energy is used to choose the leader, yet it is statistically very secure.

For example, the proof-of-work consensus mechanism devised for Bitcoin, which allows all nodes comprising the Bitcoin network to ensure they possess the same copy of the distributed ledger, is effective, but it is also extremely resource and energy-intensive and cannot scale.

Unlike other blockchain networks, temtum does not restrict block size by design. The removal of block size limits ensures that there is no theoretical limit to the number of transactions per second that can be processed.

The temtum network requires very little energy to run and this results in extremely low to zero-cost transactions. This eliminates the need for nodes to compete amongst each other, thereby removing the need to incentivize miners and preventing the centralization of specialized mining hardware pools.

How the Consensus Algorithmworks

In the temtum Consensus Algorithm, we define a small subset of nodes which function as semi-trusted authority nodes. The number of semi-trusted authority nodes is scaled with network load. The function of semi-trusted authority nodes within the temtum ecosystem can be compared to the presence of similar nodes in the Tor decentralised peer to peer privacy network, which uses 'directory authorities.'

Each authority node possesses a secret long-term 'authority identity key,' which is used to sign 'key certificate' documents. Each individual key certificate contains a medium-term 'authority signing key,' which is used by the semi-trusted authority node to sign other directory information.

These authority nodes compile node descriptors into a single document called the Node Participation Document (NPD). Authority nodes collectively verify the integrity of each individual NPD, ensuring that they are identical and contain the same nodes, IP addresses and other data. The NPD is only published once a majority of authority nodes reach consensus on the state of the document. In the event of a disagreement, a majority decision is required in order to define the NPD.

The NPD is critical in the process that results in the selection of the leader node. As every node participating in the temtum network possesses a copy of the NPD, each node is able to select the leader without reference to or querying any other node or central authority. Each node must maintain a copy of the NPD and can be queried for it at any time in order to reduce the load on authority nodes.

The nature of cryptography involved in NPD maintenance ensures that only authority nodes are able to alter the NPD. Therefore, the NPD is safe to distribute to all nodes. The NPD can only be altered by a majority of authority nodes. Any other changes made to the NPD will be rejected by the temtum network due to our cryptographic protocol implementations.

In current blockchain networks, nodes must use a centralized, trusted hard-coded server called DNS in order to find other nodes on the network. When querying the DNS server, nodes receive a list of the IP addresses of other nodes on the network. This system, however, does not monitor these nodes in any way, making it possible for network participants to inject a malicious node into the network.

There is extensive research documenting the security flaws present in the DNS system[5]. As well as the security threat posed by reliance on the DNS system, its presence in the system architecture of a blockchain network such as Bitcoin – which is generally regarded as fully decentralised – is, in reality, a centralized control element.

The temtum NPD is limited by a finite time during which it is valid. This limited validity ensures that nodes possess the most up-to-date version of the document, which is essential in determining the node that will confirm blocks for the 60-second window in which it is the leader. If the NPD is out of date, nodes may use incorrect data to select a node that is not a valid leader. In this eventuality, any transactions sent to an invalid leader would not be included in the next block.

The temtum Consensus Algorithm includes code that ensures nodes receiving valid transactions will automatically forward them to the current leader node. Only the valid leader node should be receiving transactions – any other node that is not the current leader receiving valid transactions will assume the transaction has been sent in error.

[5] Atkins, D. and R. Austein, 'Threat Analysis of the Domain Name System (DNS)', RFC 3833, DOI 10.17487/RFC3833, August 2004, https://www.rfc-editor.org/info/rfc3833 and Suranjith Ariyapperuma and Chris J. Mitchell, 'Security vulnerabilities in DNS and DNSSEC' DOI 10.1109/ARES.2007.139 23 April 2007 https://web.mit.edu/6.033/www/papers/dnssec.pdf

NPD Process

1. All nodes are required to be known by the authority node.
2. At random points in time the authority nodes test the node is alive and send/receive messages.
3. The NPD is created. This contains amongst other things the public key and IP address of the node.
4. The NPD is sent to all nodes on the network and is needed for the use of the Consensus Algorithm.

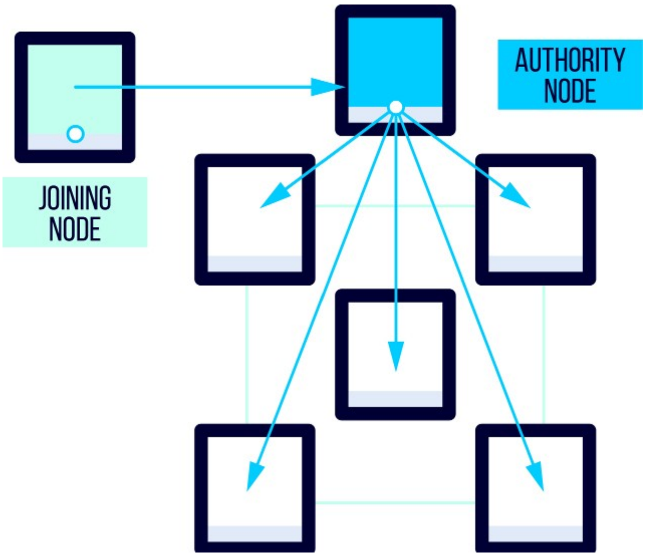


Fig 6: Join the NPD

Every temtum Node Participation Document possesses a 'valid-after' (VA) time, a 'fresh-until' (FU) time and a 'valid-until' (VU) time. VA must precede FU, which must, in turn, precede VU. Times are selected to ensure that every consensus will remain 'fresh' until the next consensus becomes valid, and 'valid' for a period of time after. At least three consensuses are valid at any given time – historic, current, and future. In the case that only one consensus is valid, the temtum network will continue to use the most recent live consensus even in the case of validity expiration, as the 'freshness' of the document is not critical and not a vector for attack.

A democratic transaction protocol

A further advantage is that network users cannot attack the network through simply buying hashing power. Proof-of-work blockchains such as Bitcoin allow network participants to pay a higher transaction fee in order to increase the likelihood that a transaction will be included in the next block. This potentially excludes lower valued transactions from the next block and increasing transaction times. The temtum network, by contrast, treats all transactions with equal priority, with advantages directly affecting the entire network where no miner rewards = no need for transaction fees.

Removing the possibility offorks

Most importantly, the temtum Consensus Algorithm removes the possibility of a fork in the blockchain. All nodes participating in the temtum network – from large-scale server-based nodes to smartphone nodes – could be selected to be the next leader and all nodes on the network can independently determine the leader based on the NIST beacon and NPD.

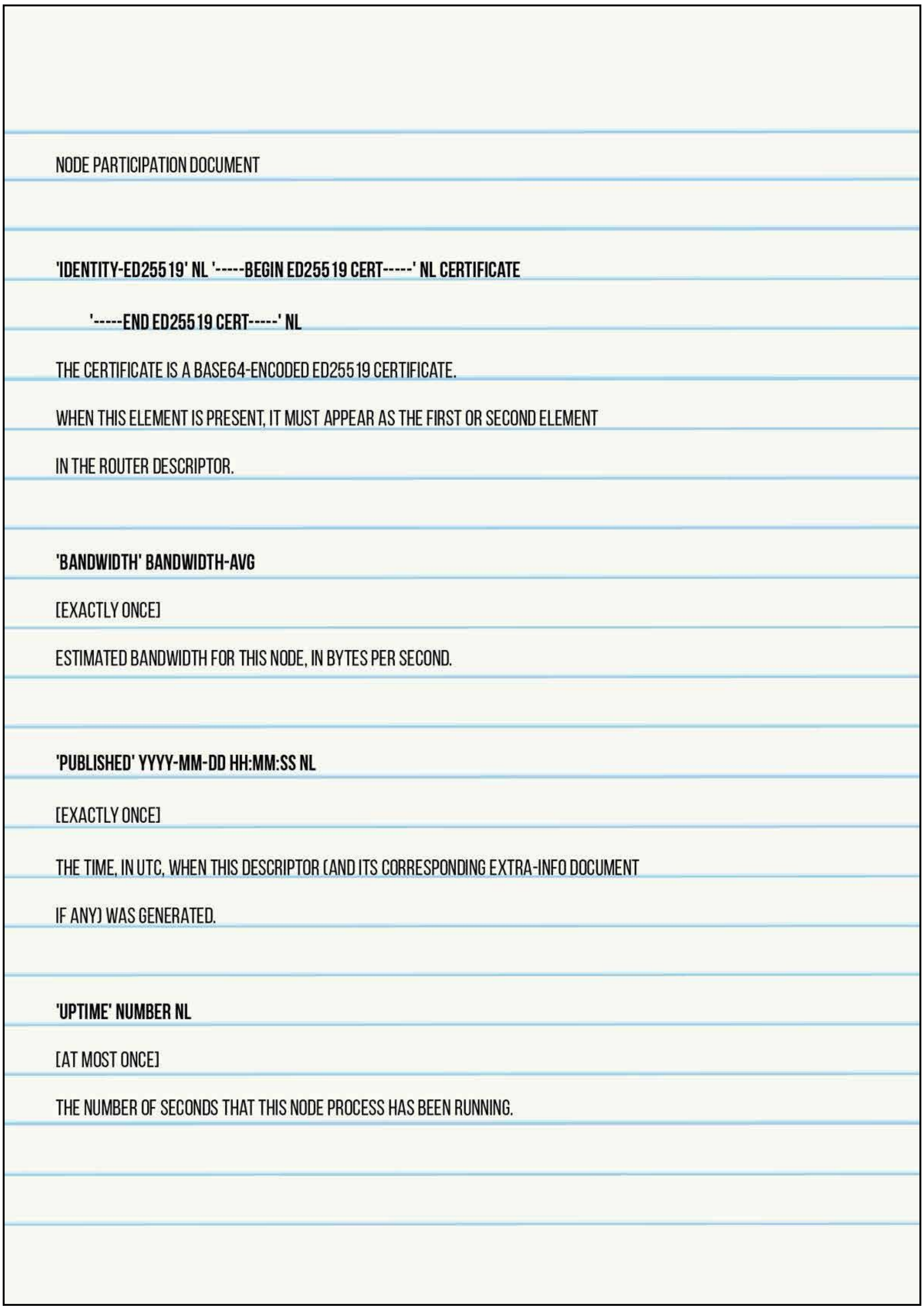
Other networks experience forks when two nodes become the leader at the same time, by solving the proof of work algorithm simultaneously causing forks resulting in double-spend, temtum rejects all blocks submitted to the network that have not been cryptographically signed by the singularly defined leader. This solution is unique and proprietary to temtum.

Node descriptor format

Each node is represented in the NPD by a descriptor which summarizes the node, their public identity, their uptime and bandwidth. This is a more detailed description of that format.

Node descriptors consist of the following items:

- **Node 'nickname' (must be a valid router nickname)**
- **Node 'IP Address' (must be an IPv4 address in dotted-quad format)**



NODE PARTICIPATION DOCUMENT

'IDENTITY-ED25519' NL '-----BEGIN ED25519 CERT-----' NL CERTIFICATE

'-----END ED25519 CERT-----' NL

THE CERTIFICATE IS A BASE64-ENCODED ED25519 CERTIFICATE.

WHEN THIS ELEMENT IS PRESENT, IT MUST APPEAR AS THE FIRST OR SECOND ELEMENT

IN THE ROUTER DESCRIPTOR.

'BANDWIDTH' BANDWIDTH-AVG

[EXACTLY ONCE]

ESTIMATED BANDWIDTH FOR THIS NODE, IN BYTES PER SECOND.

'PUBLISHED' YYYY-MM-DD HH:MM:SS NL

[EXACTLY ONCE]

THE TIME, IN UTC, WHEN THIS DESCRIPTOR (AND ITS CORRESPONDING EXTRA-INFO DOCUMENT

IF ANY) WAS GENERATED.

'UPTIME' NUMBER NL

[AT MOST ONCE]

THE NUMBER OF SECONDS THAT THIS NODE PROCESS HAS BEEN RUNNING.

General block validation

Once a block leader has been selected, it will confirm transactions for the next 60 seconds. Unlike proof-of-work blockchain networks such as Bitcoin, which confirm transactions that have previously been collected, the temtum network selects a block leader as a precursor to transaction confirmation within the period in which they are leader, in order to achieve the highest transaction throughput possible. Block leaders confirm transactions in 60-second windows in order to match the frequency at which the NIST Randomness Beacon is refreshed.

Our analyses of Bitcoin, Ethereum, and other blockchain networks have demonstrated that the optimum time frame for block generation in a decentralised network is 12 seconds. This timeframe is sufficient for 95% of the network to obtain all block data, including validation and confirmation. temtum's approach to network topology and authority nodes is novel, but it is able to send transactions to the block leader, confirm, and receive blocks within a 12-second time frame.

The 12-second block generation window makes each block leader responsible for generating 5 blocks. As with all blockchain systems, each block includes a hashed reference to the previous block inside the current block, establishing an immutable chain.

3) The Optimized Routing Algorithm

The way in which nodes within the temtum network are rapidly able to identify the current leader node eliminates the need for gossip protocol solutions for the distribution of transactions. Gossip protocols, as used in current generation blockchain networks, rely on spamming transaction information to every node in a network – regardless of whether the receiving node has already received it or not. During our testing of the Bitcoin network, each node witnesses an average of 18 duplicates of the same transaction.

This method of transaction communication results in data duplication and wasted bandwidth, slowing transaction throughput and wasting resources.

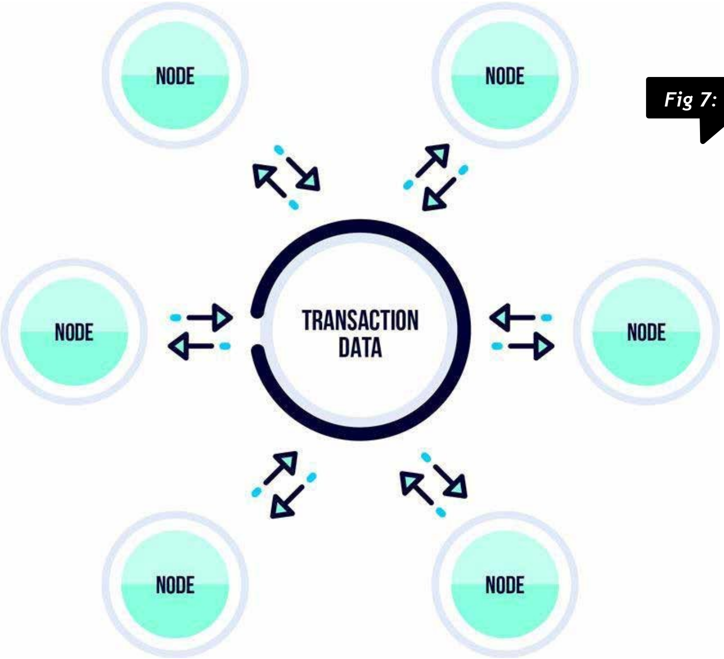


Fig 7: Gossip protocol graphic

With the temtum protocol, any node that creates a transaction sends it only to the block leader, ensuring no additional work must be performed by other nodes in the network.

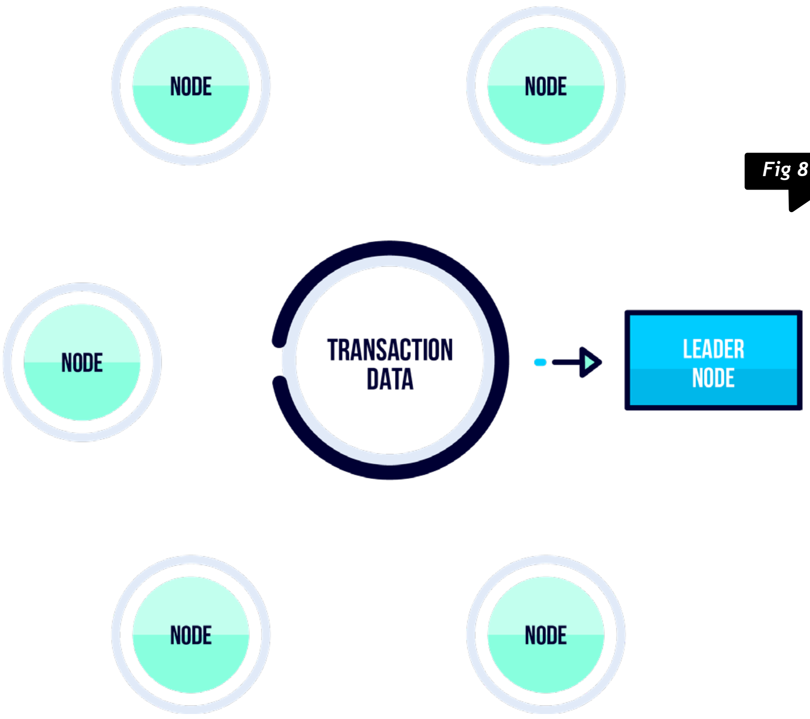


Fig 8: temtum protocol

Leader nodes are only required to receive a transaction, confirm the validity of a transaction and append it to the block.

The only computationally intensive task performed by leader nodes is transaction validation, which is performed by searching the blockchain to ensure the user has the rights and correct funds to make the transaction, and then creating a hash of the block subsequent to confirmation of all transactions, every 12 seconds within the 60-second block leader window.

This unique block validation process allows for computation to be performed on low resource devices such as smartphones – and is no more computationally intensive than other typical applications running on smartphones.

4) Random number generation and the NIST Beacon

temtum is the first cryptocurrency to commercially deploy a successful implementation of a random number generated by the NIST Randomness Beacon. Combined with the unique temtum Consensus Algorithm, this removes the need for energy-intensive proof-of-work consensus and eliminates the possibility of a fork in the blockchain, or a double-spend.

The quantum attack-resistant architecture of the temtum network uses a beacon broadcast by the US Department of Commerce National Institute of Standards and Technology (NIST) to generate random numbers that cannot be algorithmically predicted. The NIST Randomness Beacon[6] uses quantum effects to generate a truly random number once every minute. This random number is used as the basis to select the node that will confirm transactions on the temtum network for the subsequent minute.

temtum also features multiple, automatically started quantum effect fallback options should the NIST Beacon ever not broadcast a value 60 seconds after its last output value. This ensures that the use of true random number generation via third-party technology will never result in any network downtime.

[6] https://www.nist.gov/programs-projects/nist-randomness-beacon

The NIST Randomness Beacon is a source of truly random numbers that broadcasts full-entropy bit-strings in blocks of 512 bits every 60 seconds, providing three key functions: unpredictability, autonomy and consistency.

The unpredictable nature of the NIST Randomness Beacon makes it impossible for any user to predict the bits it generates before they are published by the source. All users accessing the source of the beacon can be confident that they all receive an identical random string, while the beacon remains highly resistant to malicious interference by external parties.

The key features of the NIST Randomness Beacon include:

- **Generated numbers that cannot be predicted before they are published – even by future quantum computing techniques.**
- **The public, time-bound and authenticated nature of the NIST Randomness Beacon allows any user application to prove that it used truly random numbers not known before a specific point in time.**
- **Proof of random number generation can be validated offline at any point subsequent to generation.**

Based on these properties, the NIST beacon has been chosen as a source of randomness for the Temporal network.

How the NIST Randomness Beacon works

The NIST Randomness Beacon generates random numbers using a process that is based entirely on quantum mechanics. It means that it is able to generate a value that is truly random to a degree that has never before been achieved in computing.

The method through which the NIST Randomness Beacon generates random numbers is distinct from the algorithmic random number generators that are in use today – while traditional methods can pass statistical tests for randomness, they rely on software algorithms that operate on physical devices that are subject to deterministic physics.

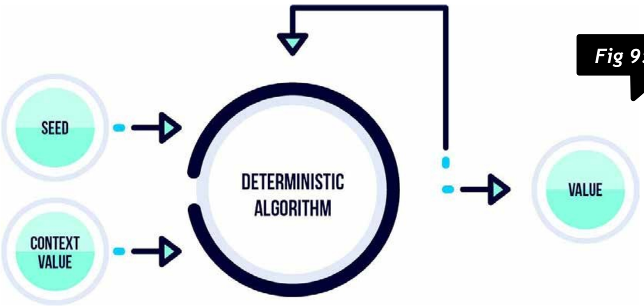


Fig 9: Existing method graphic

'Random' numbers generated via algorithmic random number generators rely on classical physical principles or operations that cannot be certified as absolutely unpredictable. The NIST Randomness Beacon, however, operates on a method developed in partnership with the physicists from the NIST Physical Measurement Laboratory that generates random numbers through the testing of photonic states.

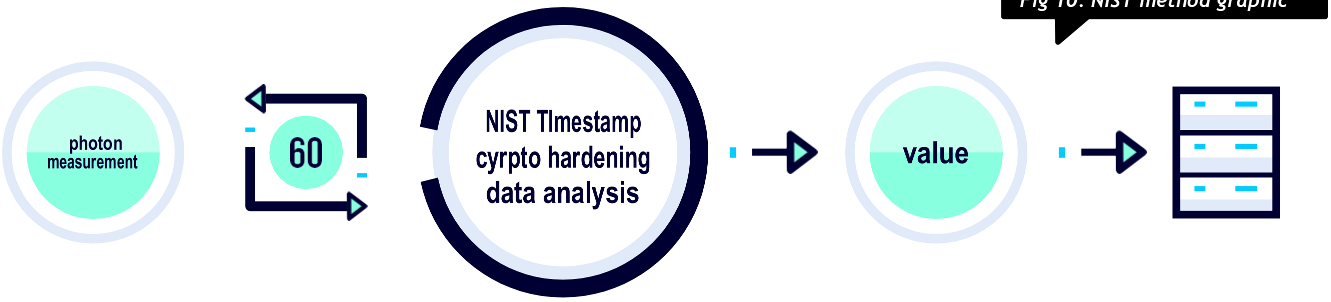


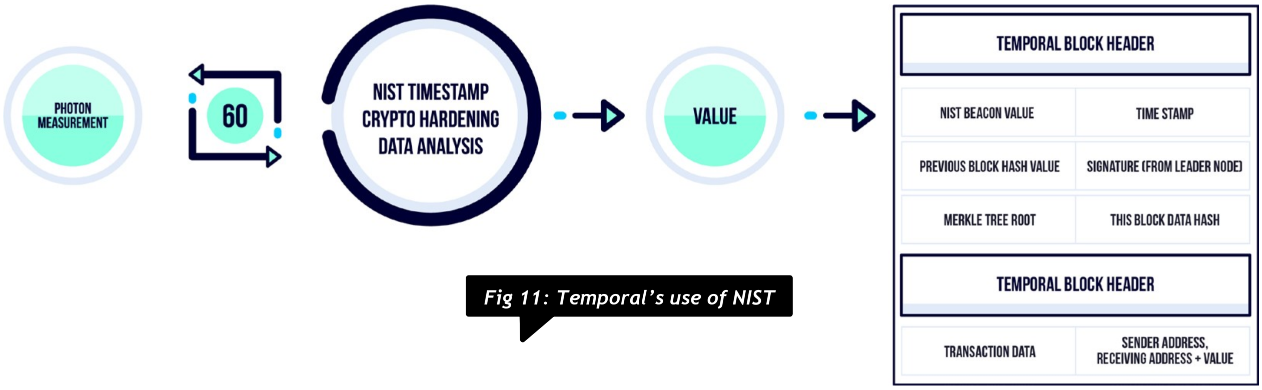
Fig 10: NIST method graphic

The Beacon builds on methodology established by the NIST in a 2015 Bell test[7] that confirmed the existence of the quantum entanglement effect that Albert Einstein called: 'spooky action at a distance.' Before observation or measurement, a particle exists in a 'superposition' of possible states. Observation forces it to manifest specific properties, the recorded values of which are purely probabilistic.

NIST Randomness Beacon security

We use the NIST Randomness Beacon in the temtum Consensus Algorithm and as a timestamp in block generation.

In our model the timestamp is the truly random NIST Randomness Beacon Value, which is generated every 60 seconds. This eliminates the possibility that a malicious party could pre-compute the timestamp value – for a block to carry the NIST Randomness Beacon timestamp, the block must have been generated subsequent to the release of the value from the beacon. Thus, we can be certain that an 'offline chain attack,' which can be conducted on other blockchain networks, cannot be executed on the temtum network.



TEMPORAL BLOCK HEADER

NIST BEACON VALUE	TIME STAMP
PREVIOUS BLOCK HASH VALUE	SIGNATURE (FROM LEADER NODE)
MERKLE TREE ROOT	THIS BLOCK DATA HASH

TEMPORAL BLOCK HEADER

TRANSACTION DATA	SENDER ADDRESS, RECEIVING ADDRESS + VALUE

Fig 11: Temporal's use of NIST

The degree of randomness in the values generated by the NIST Randomness Beacon dramatically increases the cost of an attack directed at the temtum network by orders of magnitude greater than current cryptocurrencies.

Numbers generated by the beacon cannot be predicted by any means before they are published. The public, time-bound and authenticated nature of the NIST Randomness Beacon allows user applications to prove that the truly random numbers it uses are not known before a specific point in time. This proof can be presented offline at any point subsequent to broadcast. For example, the proof could be mailed to a trusted third-party, encrypted and signed by an application, and only opened if needed and authorized.

[7] A strong loophole-free test of local realism: Phys. Rev. Lett. 115, 250402 (2015): https://arxiv.org/abs/1511.03189

For a 512 key by definition there are 2^{512} possible keys to 512-bit cypher, and in a well-defined cypher, all keys are equally strong.

Technically, a cypher is a bijective mapping between cleartext and plaintext, so for a given cypher with 512 bits this equals 2^{512} bijective mappings.

Consider the set of texts of length N bits – there are 2^N different texts possible. The tensor product is the set of all possible combinations of N bit vectors of text and 512-bit vectors of key, the size of which is:

$2^N * 2^{512} = 2^{N + 512}$

Unlike deterministic computers, which encode data in binary digits – each of which is always in one of two definite states, 0 or 1, quantum computers use quantum bits or qubits, which can be in a superposition of states. Quantum computing development is accelerating rapidly – IBM published evidence of robust quantum computation capacity in late 2017[8], and unveiled new fault-tolerance capabilities that have helped to scale quantum processors beyond 50 qubits[9].

Current estimations for an implementation of Grover's algorithm for AES requires far more qubits than current quantum machines possess. Grassl et al. states that the required number of qubits required to implement an exhaustive key search for AES-256 is 6681[10].

It is not unreasonable to draw similar conclusions for SHA2-512, which has a far larger internal state, and postulate that 1024 qubits are not enough. Research investigating the cost of generic quantum preimage attacks on SHA-2 demonstrates that such an attack would require 212.6 logical qubits[11]. Since the NIST Randomness Beacon generates values using SHA2-512, it is reasonable to assume the same level of resources are required.

Even with modern day, or even near-future quantum machines, it is still a massive leap to brute-force 512-bit keys. To do so within the 60-second window as used by the NIST Randomness Beacon is statistically infinitesimally improbable – approximately the inverse of 2^{512}. In short, the probability of correctly guessing the NIST beacon 512-bit key ahead of time is almost certainly zero, making it highly secure.

Implementing NIST

Two independent hardware random number generators are used to generate 512 bits of randomness, which are then subjected to an XOR logical operation together to yield the seed value. This number alone is an extremely secure 512-bit random number.

The seed value is then collected, together with relevant descriptive data, which comprises: a version number, frequency of output, timestamp, chaining status code and the value of the previous output. This process correlates the random outcome with the time it was created, as well as linking this value with the previous value. The collection of data is then hashed with SHA-512 and signed with the NIST Randomness Beacon's private key, yielding the signature.

Given the NIST Randomness Beacon public key, it is easy to verify that the signature corresponds to the relevant data and has been signed by the beacon.

The signature is then hashed with SHA-512 again in order to create the final output value, which is used as the random number. This value incorporates all the information relevant to this 60-second window as it is a hash of the signature which, in turn, is a hash of the data. The hashing process

[8] Experimental Demonstration of Fault-Tolerant State Preparation with Superconducting Qubits, IBM T.J. Watson Research Center, Phys. Rev. Lett. 119, 180501 https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.119.180501

[9] Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits, https://arxiv.org/abs/1710.05867

[10] Applying Grover's algorithm to AES: quantum resource estimates, https://arxiv.org/abs/1512.04965

[11] Estimating the cost of generic quantum preimage attacks on SHA-2 and SHA-3, https://arxiv.org/pdf/1603.09383.pdf

preserves the original entropy of the seed value but ensures that the output value depends on the NIST Randomness Beacon secret key and all relevant background data in a way that can be verified.

In contrast, 'random' numbers generated via algorithmic random number generation are not certifiably random due to their dependence on software or hardware – while statistical analysis may yield results that imply randomness, algorithmic random number generation cannot be absolutely guaranteed to yield true random numbers and is susceptible to tampering.

The NIST Randomness Beacon delivers a superior source of randomness, using a physically observable manifestation of the wave nature of quantum systems to generate fundamentally unpredictable results.

NIST Randomness Beacon output can be certified to be truly random even if the measurement settings and seed are publicly known. The only requirement for true random certification is that the Bell test used to confirm that the phenomenon generating the numbers is entirely quantum mechanical and is free from tampering and interference.

temtum NIST Integration

The NIST Randomness Beacon publishes a new certifiably random value to the internet every 60 seconds. Each temtum node is required to download the latest 512-bit random number published by the Beacon. If, for any unforeseeable reason, the NIST Randomness Beacon does not transmit a new value, the temtum network will continue to use the most recent value. The NIST Randomness Beacon has operated continuously since launch, however – no failure to transmit has occurred.

All nodes participating in the temtum network will access the NPD created by authority nodes independently. The NPD contains a list of all nodes on the network, their IP addresses, and their identity in the form of a public key. All nodes are able to select the next leader node independently but will end up with the same leader node by design.

The leader node is determined by taking the first 256 bits of the NIST Randomness Beacon timestamp and subtracting the individual public key values of all nodes on the network. The node that yields the result closest to zero – whether positive or negative – will become the leader node for the next 60-second window.

But not all nodes are considered in the leader selection process. To be considered for leader selection, a node must have a valid flag that identifies them as an eligible leader node based on the NPD. All nodes have the same NPD, which is updated on an hourly basis.

The probabilities of determining NIST Values

The NIST Randomness Beacon generates a random number in blocks of 512 Bits every 60 seconds. This process is performed by first generating 2 random numbers from two independent sources.

Figure 1 describes the process that the NIST Randomness Beacon follows.

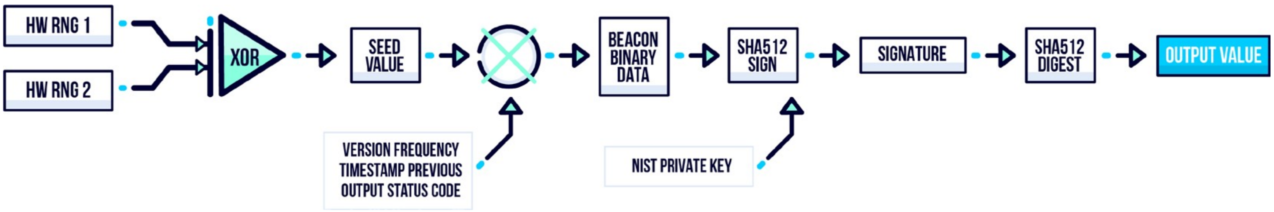


Fig 12: NIST Randomness Beacon Process [12]

[12] Latinov, L. (2018, May 03). MD5, SHA-1, SHA-256 and SHA-512 speed performance. Retrieved from https://automationrhapsody.com/md5-sha-1-sha-256-sha-512-speed-performance/

In order to obtain the final output value, we need to know:

- **HW RNG1: (Private data) the first random number generated by independent hardware.**
- **HW RNG2: (Private data) the second random number generated by independent hardware.**
- **Version, Frequency, Timestamp, Previous Output, Status Code: Public data that can be found at https://beacon.nist.gov/home**
- **NIST Private Key: the private key used to hash the data.**

The time to obtain the output value before the NIST Randomness Beacon publishes it, must follow the formula:

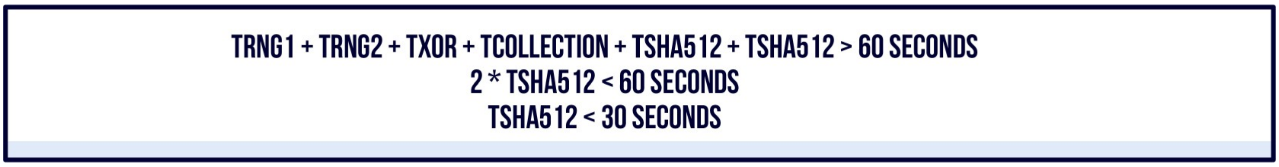
tRNG1 + tRNG2 + tXOR + tCollection + tSHA512 + tSHA512 < 60 seconds

Fig 12: Formula for NIST Beacon generator

Where:

- **tRNG1 and tRNG2 represent the time taken to generate the first and second random number. They must likely be the same and we will assume 0.**
- **tXOR is the time spent to XOR the HW RNG1 and HW RNG2. For the purpose of the project, we will assume is 0.**
- **tCollection is the time spent to collect the Seed Value with the version, frequency and so on. For the purpose of the project, we will assume is 0.**
- **tSHA512 is the time spent to hash the data.**

Therefore, the formula states as:



TRNG1 + TRNG2 + TXOR + TCOLLECTION + TSHA512 + TSHA512 > 60 SECONDS
2 * TSHA512 < 60 SECONDS
TSHA512 < 30 SECONDS

Fig 13: Time-Formula for NIST Beacon generator

Latinov (2018) experiments[13] show that tSHA512, using 1 core of an Intel i7 2.60 GHz and 16GB of RAM, is approximately 1 second. Therefore, we need at least 1 second per number generated. This equates to 30 attempts in 60 seconds in order to verify that we guessed the output value correctly, assuming that we managed to previously obtain the NIST private key.

Although the time is relatively high, we still need to generate the exact 2 random numbers the NIST Randomness Beacon will use at the beginning of the process.

[13] Latinov, L. (2018, May 03). MD5, SHA-1, SHA-256 and SHA-512 speed performance. Retrieved from https://automationrhapsody.com/md5-sha-1-sha-256-sha-512-speed-performance/

The probability of finding one number in n attempts is:

Fig 15: Probability of 1 random number

$$\text{PROBABILITY (1 NUMBER)} = n^* \frac{1}{\text{Nitems}}$$

n = NUMBER OF ATTEMPTS
Nitems = NUMBER OF POSSIBLE NUMBERS

$$\text{PROBABILITY (2 INDEPENDENT NUMBERS)} = n^* \frac{1}{\text{Nitems}} * \frac{1}{\text{Nitems}}$$

n = NUMBER OF ATTEMPTS
Nitems = NUMBER OF POSSIBLE NUMBERS

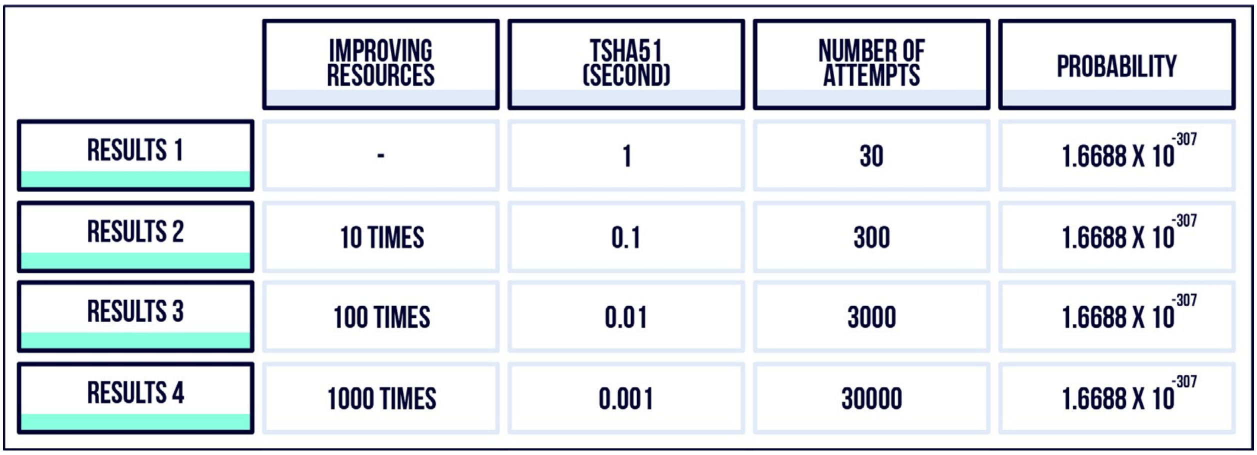
Fig 16: Probability of 2 exact (independent) random number

By definition, there are X possible numbers in 512 bits and, as stated before, we have 30 attempts, so;

$$\text{PROBABILITY (2 INDEPENDENT NUMBERS)} = 30^* \frac{1}{2^{512}} * \frac{1}{2^{512}} \cong 1.6688 \times 10^{-307}$$

Fig 17: Probability of 2 exact (independent) random number of 512 bits on 30 attempts

Even if the attacker is able to multiply the resources directed at the attempt 10, 100, or 1000 times, the probability does not meaningfully improve:



	IMPROVING RESOURCES	TSHA51 (SECOND)	NUMBER OF ATTEMPTS	PROBABILITY
RESULTS 1	-	1	30	1.6688 X 10^{-307}
RESULTS 2	10 TIMES	0.1	300	1.6688 X 10^{-307}
RESULTS 3	100 TIMES	0.01	3000	1.6688 X 10^{-307}
RESULTS 4	1000 TIMES	0.001	30000	1.6688 X 10^{-307}

Fig 18: Probabilities with increased resources

There is virtually no probability of accurately predicting the exact two 512-bit random numbers generated by the NIST Randomness Beacon within the 60-second window of opportunity, even given vast resources.

The above calculation analyses the task of predicting the NIST Randomness Beacon output in advance. In order for the prediction to assist in the execution of an attack, however, an attacker would need to control the specific node that possesses a public identity that, when computed with the NIST Randomness Beacon value, is closest to zero on the network. This can be defined as Y/X where Y is the number of nodes the attacker has control of, and X which is the network size.

Ultimately, a pre-computational attack on the temtum network is impractical and, as demonstrated, would result in zero impact on the network even if a malicious actor is able to successfully execute an attack.

Blockchain networks that rely on the proof-of-work consensus model present malicious actors with the opportunity to withhold the solution to the proof-of-work algorithm and gain an unfair advantage on the next block. An attacker with sufficient resources targeting a proof-of-work blockchain can consistently outpace the network.

The temtum network, however, leverages a source of randomness that cannot be pre-computed, and this ensures that there is no method of using the current block as a mechanism for predicting future blocks.

Overall temtum network architecture

1. **The Node Participation Document (NPD) is created by the authority node and is sent to all nodes on the network.**

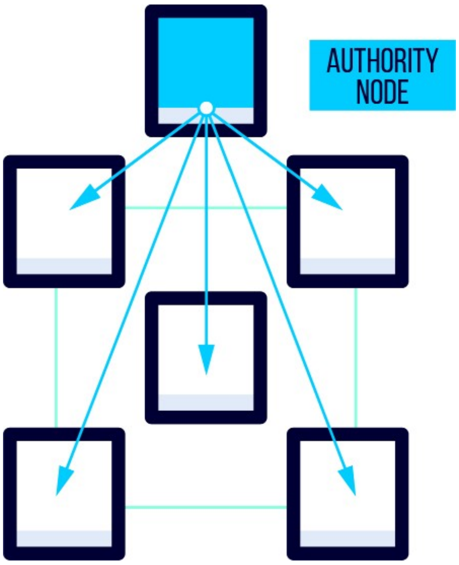


Fig 19: Sending NPD to the nodes

2. **All nodes query the NIST beacon every 60 seconds and obtain the latest value.**

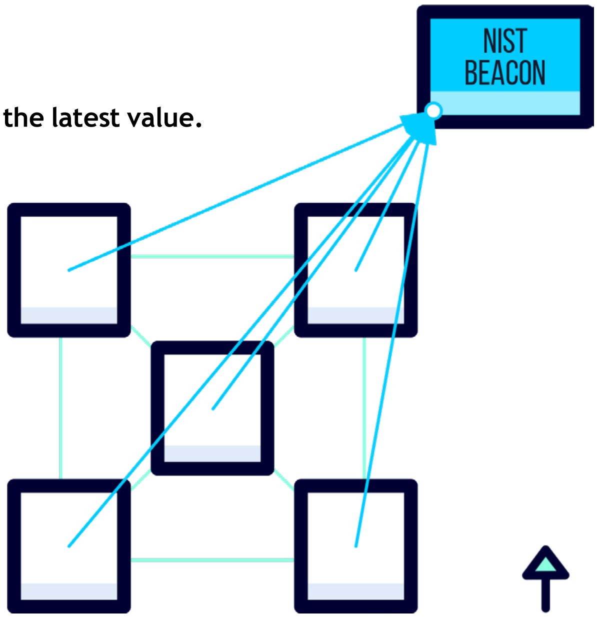


Fig 20: All nodes query the NIST beacon

3. All nodes determine the leader node.

   - This is done locally, but critically all nodes will come to the same answer.
   - All nodes deduct the beacon value for the public node identity (stored within the NPD).
   - The node whose value is closest to zero becomes the leader.
   - There is no need to query any other node.

   - The leader is now selected and has write access to the blockchain for the next 60 seconds and 5 blocks.

4. All nodes directly send TX's to the leader node – this is done for one minute before the process of selecting a new leader is repeated.

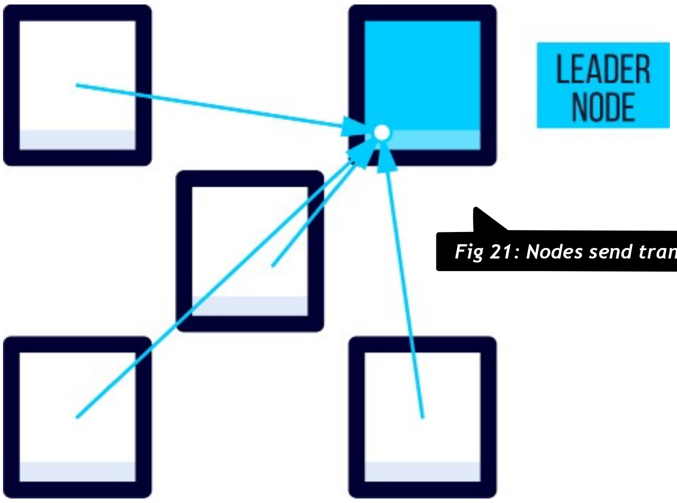


Fig 21: Nodes send transactions to the leader node

5. The leader node receives TX's and:

   - Checks if the TX is valid
   - Checks local copy of the nodes blockchain
   - If not in local copy – query archive node
     - If archive node replies valid confirm TX into block
     - Else reject
   - Blocks are created every 12 seconds
     - Header contains NIST beacon value
     - Hash of all TX's in block
     - Previous hash of previous block

Each leader node is responsible for five blocks (5 x 12 Seconds per block). Five blocks contain the same NIST beaconvalue.

The block structure comprises:

- Previous block hash
- NIST value
- Hash of all TX's
- Time stamp
- TX's
- Signed by the leader node

6. The block is sent to all nodes.

   - The leader node then presents the block to the network.
   - All nodes individually check that the block is valid.
   - Checks the signing node was the leader node.
   - If valid, this appends this block to the node's local copy of the blockchain.

Resilience to attack

The temtum network architecture is by design immune to a 51% attack, so the majority of attack vectors which have developed to target Bitcoin and similar networks are not a threat to the temtum network.

Since it is possible for all nodes to know which node will be responsible for creating a block ahead of time, and there is only ever one node which can produce a block each minute, there is no situation in which a fork in the blockchain can occur, eliminating the possibility of a double-spend attack.

Unlike other cryptocurrency networks which are affected by a multitude of attacks, our most serious threat is a Sybil attack in which an attacker floods the network with malicious nodes in order to disrupt the network, slowing network transactions or preventing transactions being processed, thus damaging the credibility and value of the network. However, the current network architecture of the temtum network ensures attack by malicious nodes is not possible. At present, only pre-approved nodes can participate on the network, which has been done to reduce the attack vector of a potential attacker during growth of a new network.

In our technical roadmap we give details of our intended implementation of a reputation system, called the Performance Integrity Protocol (PIP), which will allow for other users to act as a node and for the network to determine the suitability of whether each node should participate on the network without any need for a trusted third-party or central authority.

We calculate that our PIP system would require extremely high setup costs from malicious attackers to be able to contemplate a 51% attack against the temtum network – with no guarantee of success. This means that our network is a factor of over 4,000 times more resistant to attack than current cryptocurrencies based on mining, assuming a 6-month delay until successful completion caused by our road mapped Performance Integrity Protocol.

We have considered what might occur in a hypothetical attack on temtum after a bad actor has become a node on the network. If such a hypothetical malicious node should choose to attack the temtum network – regardless of economic and time-loss – the attacker will still need to be randomly chosen as a leader from the completely random nature of the NIST Randomness Beacon to confirm transactions. Should the attacker acquire 51% of the nodes on the network, then they would be chosen to be the leader the majority of the time.

However, even when the malicious node is chosen as leader and confirms artificial transactions crediting the attacker's account with a larger balance, the historical data means that when the attacker attempts to spend the newly credited amount, the next block leader will not accept the transaction.

All nodes on the temtum network are able to determine which node created the artificial transaction. This means that the malicious node will not be eligible for block leader status after its removal from the NPD.

The temtum network does not rely on mining, and therefore is not susceptible to the same 51% attacks that proof-of-work networks such as Bitcoin are open to, in which an attacker that controls sufficient hashing power is able to recreate a valid blockchain with an extensive block history.

Real World Applications

temtum

Cryptocurrency. Evolved.

Many cryptocurrencies feature lots of fantastic theoretical work, but when it comes to integrating them into real-world systems, they are severely limited. temtum, though, has already been deployed and tested, demonstrating that our theoretical solutions to blockchain problems are also effective in reality. After all, what's the point of owning cryptocurrency if you cannot use it? This section focuses on four main forms of real-world integration, in which temtum is used as a:

1. medium of exchange;
2. point-of-sale (PoS) mobile payment solution to enact the medium of exchange;
3. currency within online gaming applications;
4. e-commerce payment application;

Each user can have a temtum wallet where they can store and manage their TEM. This will be accessible both as a web app and a smartphone app. We have also developed additional functionality including a bespoke temtum keyboard for smartphone integration, which features a temtum button that enables users to send temtum from one account to another without opening the temtum app. Refer to the 'Network Integration' section for more details.

temtum as a medium-of-exchange cryptocurrency

The original cryptocurrency, Bitcoin, does have a use case and serves a recognized function as a non-fiat alternative currency that aims to provide an electronic payment system based on cryptographic proof rather than trust, which means that any two parties can transact with one another without needing a trusted third-party. But the flaws inherent in the Bitcoin system mean that it has limited application as a medium of exchange.

We want to allow all users to fully participate in the temtum network regardless of the resources they are able to contribute. The temtum network has been designed from the ground up to run at full capacity on low-powered devices such as smartphones or IoT devices. The only prerequisite to network participation access to an active internet connection or an SMS connection.

The original prototype temtum network has been fully deployed and functional on a wide range of devices that include low power personal computers, servers, basic android mobile devices, and even a smart car – a BMW i8.

Prototype network performance analysis demonstrates that temtum is able to operate at high speeds despite the varying computational and storage capacity of the resources available to it and deliver higher transaction throughput while using less computational power and energy than alternative proof-of-work blockchain networks such as Bitcoin.

TEM currency features

temtum has a number of key characteristics that makes it ideally suited as a medium of exchange cryptocurrency. These are:

Medium-of-exchange characteristics:

- **Divisibility – sub-divisible into small units**
- **Convenience – ultra-fast, with zero embedded transactions fees/costs**
- **Ease of adoption – the network can function on low-powered devices, enabling widespread network access over time**

Divisibility

Each temtum is coded to be sub-divisible into 10 to the power of 8 units with fractional levels capable of being described by technical nomenclature.

This sub-divisibility allows capacity for global dissemination of temtum as an alternative currency, whilst still maintaining the ability to execute fractional trades of a single US cent equivalent.

Convenience

- **Ultra-fast blockchain.**
- **Simulated transaction throughput speeds of 120,000 transactions per second demonstrated in a laboratory environment.**
- **Positive scaling effect – increases in network adoption result in faster network speeds by employing sharding and delegation as described in the roadmap section of this document.**
- **Zero embedded transaction fees/costs.**

Ease of adoption

The temtum network can be run on low-powered devices such as smartphones, and temtum itself can be transferred via SMS text message on non-smartphone mobiles, enabling widespread adoption over time.

Durability

temtum's use of the Temporal Blockchain and temtum Consensus Algorithm does not require Proof of Work mining or resource intensive computing power. The network is scalable over time as data is sent to archive nodes periodically, maintaining a stable blockchain size with no scaling issues

on memory usage. It is also energy efficient and environmentally friendly, using just a fraction of the resource / energy of previous blockchains cryptocurrencies. temtum network cryptography is highly resistant to attack via quantum computing.

Conclusion

Given the medium-of-exchange characteristics (divisibility, convenience and ease of adoption) set out above – and in more detail in the 'Technology' section – we believe that temtum has a strong case to act as a significantly superior alternative to existing cryptocurrencies such as Bitcoin in serving as a medium of exchange.

temtum has been specifically designed to be more durable than Bitcoin over time, with a scalable structure and at a fraction of the energy usage.

Vision for temtum as a mobile POS payment system

Integration into existing payment models

temtum's ambition to be the first cryptocurrency to achieve mass global adoption means that we have ensured that the network can fully integrate with standard, real-world payment systems. We have developed solutions for point-of-sale (POS) mobile payments, providing a seamless process for consumer retail purchases via existing mobile or contactless payment networks.

Our belief is the speed, security and scalability of the temtum network will easily allow users to spend their TEM in the conventional economy by exploiting existing technology infrastructure at minimal cost and maximum convenience. This is consistent with the vision outlined above of temtum as a mainstream medium of exchange.

Benefits

This pioneering move of integrating temtum with conventional payment systems should allow temtum to coexist transparently with other standard (fiat) currencies in the same payment ecosystems that already exist. The adoption of a cryptocurrency can be viewed in two ways:

1. 'How can it be used now?'; and
2. 'How will it be used in the future?'

The now: For any payment coin to achieve mass adoption, it must integrate into our existing financial systems, whereby every day items and transactions can be carried out as they are now, without a fundamental change to processes at any stage of the retail process. The barriers for entry are much lower by targeting payments at their source, rather than at their destination – targeting on-boarding payment gateways and financial institutions, rather than retailers, is the most effective route to adoption.

The future: Cryptocurrencies will be the future of payments. Instant, feeless, trustless and highly secure payments could be made through temtum, without requiring any institution acting as a third-party. Greater accessibility to cryptocurrencies will serve to benefit the future of payments.

TEM Mobile PoS payment solution

We intend for any user with a temtum wallet to be able to make purchases using conventional payment networks, such as Visa for instance, with total transparency to the vendor who will see only a fiat money transaction. Yet all the advantages of temtum – for example, immediate international transfer of value – will still be available.

There are a number of benefits for users (consumers) in adopting temtum as a mainstream form of payment.

They include:

- **The currency should hold consistent value across all territories and can be transferred internationally without cost.**
- **For peer-to-peer payments (for instance, if users want to split a bill with a friend), it's free and near instantaneous.**
- **Transactions take just 12 seconds compared to hours-to-days with conventional bank accounts.**

In contrast to other cryptocurrencies, our goal is to enable the use of temtum for everyday purchases, for example at major retailers. Therefore, we have developed a process which uses existing payment infrastructure which requires no modifications. It uses the NFC capability on a smartphone interacting with standard POS terminals, which are in widespread use in developed economies. The merchant is unaware that temtum is being used. (A merchant always has, if they want, the ability to receive temtum directly into their wallet, but that is not the purpose here).

The payment process can be as fast and convenient as payments using conventional currency.

Partnering with banks and/or payment cards

We are looking to engage with a range of challenger banks and payment card providers to create a digital temtum credit/debit card.

These potential partners would fully support the integration of their system with temtum. TEM would be listed on one or more exchanges to directly enable conversion of temtum to conventional currency (fiat) as part of this process.

We have already successfully developed and tested this model using an emulator for banking interfaces.

This process flow shows how users would use this in real life:

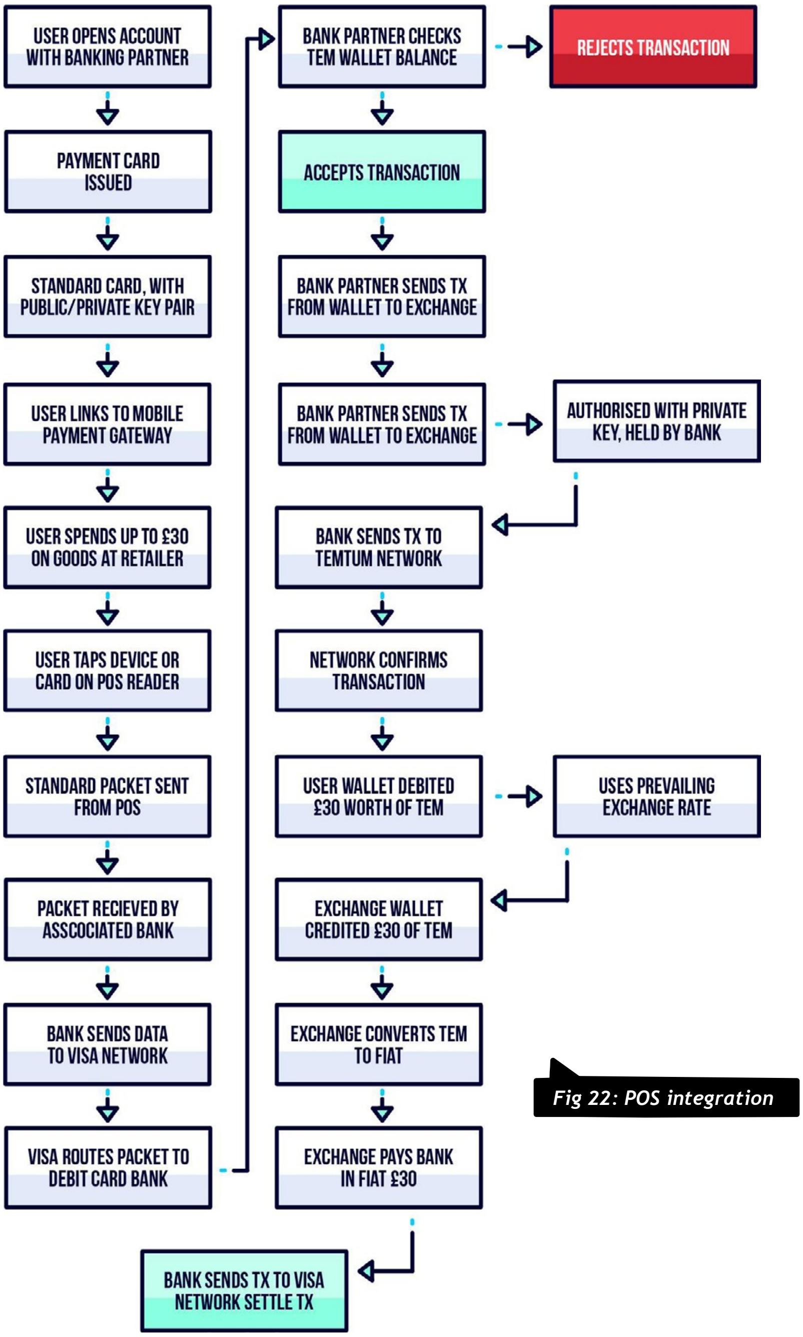

USER OPENS ACCOUNT WITH BANKING PARTNER
PAYMENT CARD ISSUED
STANDARD CARD, WITH PUBLIC/PRIVATE KEY PAIR
USER LINKS TO MOBILE PAYMENT GATEWAY
USER SPENDS UP TO £30 ON GOODS AT RETAILER
USER TAPS DEVICE OR CARD ON POS READER
STANDARD PACKET SENT FROM POS
PACKET RECIEVED BY ASSCOCIATED BANK
BANK SENDS DATA TO VISA NETWORK
VISA ROUTES PACKET TO DEBIT CARD BANK
BANK PARTNER CHECKS TEM WALLET BALANCE
REJECTS TRANSACTION
ACCEPTS TRANSACTION
BANK PARTNER SENDS TX FROM WALLET TO EXCHANGE
BANK PARTNER SENDS TX FROM WALLET TO EXCHANGE
AUTHORISED WITH PRIVATE KEY, HELD BY BANK
BANK SENDS TX TO TEMTUM NETWORK
NETWORK CONFIRMS TRANSACTION
USER WALLET DEBITED £30 WORTH OF TEM
USES PREVAILING EXCHANGE RATE
EXCHANGE WALLET CREDITED £30 OF TEM
EXCHANGE CONVERTS TEM TO FIAT
EXCHANGE PAYS BANK IN FIAT £30
BANK SENDS TX TO VISA NETWORK SETTLE TX

Fig 22: POS integration

Key points:

- **The time to confirm the transaction is the same as a standard card transaction.**
- **All original protocols and messages are kept – no need to modify packets etc.**
- **All transaction data is stored on the blockchain.**
- **No modification to the POS device is needed.**

To be developed:

- **The challenger bank will need to create a digital card with an associated temtum keypair – a small amount of work as the debit card is standard and requires only the linking of the private and public keypair to the card.**
- **The challenger bank will need to create the ability to create a transaction for temtum using already existing code.**
- **An exchange is then used to convert temtum to regular currency (fiat).**

Online gaming & Esports

Online gaming was a 135 billion USD industry in 2018[14], while esports topped an audience of 435m[15] as blockchain now attempts to disrupt the way in game payments and game assets are earned, used, stored and traded for a share of this market.

temtum allows publishers and players, as well as any other online gaming enthusiast, to enjoy their favorite pastime free of fees, payment delays and legal restrictions and offers significant advantages relative to using the likes of BTC or ETH as a form of payment. Players can 'pay-as-you-play' without the need to deposit to an applications wallet and drawdown on funds. Therefore, players will instantly transfer what they intend to bet for any single hand, stake or prediction.

Players can 'pay-as-you-play' without the need to deposit to an applications wallet and drawdown on funds. Therefore, players will instantly transfer what they intend to spend for any single asset, game or in-game purchase.

Core solutions:

- **Removing crypto deposit delay –** customers want to see their funds instantly - allowing instant purchases. Logging out and back in to see deposited funds is not a user friendly experience.
- **Instant buy backs -** with existing cryptocurrency coins, buying back into games is generally not possible without a lengthy depositing process. Therefore, continuation of the same gaming experience is not achievable.
- **Removing depositing of funds –** 'Pay as you play' gaming eliminates the risk of a gaming application holding your deposit or your assets in their wallet.
- **Instant withdrawals -** remaining deposits are immediately paid directly to your wallet in TEM, without transaction delays.

temtum is in active discussions with several esports platforms, including tournaments, with an aim to see mass-adoption across the existing esports sector. Already developed is a demonstration of how temtum will integrate with online gaming applications in the form of our card trading demo. We are targeting a minor niche of the gaming market to secure at least one million online transactions via integrations in 2019 alone.

[14] https://techjury.net/stats-about/gaming-industry-worth/

[15] https://techjury.net/stats-about/gaming-industry-worth/

There are two very different ways in which temtum can improve payments in this industry.

The first we call the ‘on-ramp’ model – this allows TEM to be used to pay in-game, either through a traditional deposit of funds or with our temtum ‘Pay as you Play’ model.

The second is a full online gaming application running on the temtum network, and is not described here or within this paper, but has already been demonstrated in our gaming demo. This option may form part of our future road map as integrations are demonstrated alongside industry partners – the benefit to the industry is that this technology offers a full audit on the blockchain, so players can see assets ownership and payment history as described by the game publisher.

Fiat on-ramp

There are four types of temtum gaming integrations that can exist in the on-ramp space:

- **Full temtum gaming app -** All transactions, and therefore any in-game asset ownership, will pass through the temtum network, instantly and forever tracked.
- **Hybrid online app -** This works like a regular game payment system, but you can deposit, play and withdraw using TEM via our payment plugin, or via an existing crypto payment processor interface.
- **Pay-as-you-play -** Instant payments in-game, with no depositing directly to the platform required. Both in-bound payments and withdrawals will be direct wallet to wallet transactions.
- **temtum payment gateway -** Working like a regular online game, but you can deposit using TEM via a payment gateway partner. Do note that most games will convert your temtum into Fiat currency such as dollar, euro etc. and you cannot withdraw temtum without another conversion.

In the example of an existing online game application wishing to accept TEM as a payment method, the game developer would simply create a temtum wallet and integrate our payment plugin into their platform. The plugin creates a unique wallet address for each player automatically at user sign up, allowing the application to easily monitor each users depositing or in-game payments – requiring no input from the user.

The game developer can then either automatically convert any TEM to fiat via an exchange or hold the amount in their TEM wallet.

The benefits of using TEM over more established cryptocurrencies such as BTC and ETHare recognised by both the players and apps alike, where current blockchain and crypto friendly platforms are still falling short of suitable solutions outside of game asset ownership.

temtum benefits players where they can directly use crypto (TEM) for in-game purchases with immediate transactions and no fees. For game publishers, unlike waiting on average 45–60 minutes for Bitcoin to confirm a transaction, potentially losing the player valuable gaming time, they will have the funds confirmed in their account within 12 seconds, retaining player engagement.

With the use of TEM for both payments and rewards, price volatility of the currency is less of a concern for the publisher, with instant transactions and no bank or payment gateway fees providing significant benefits in both the long and short term.

Via the ‘pay-to-play’ model, online gaming platforms no longer need to hold any client deposits and are therefore able to significantly reduce their own asset management risks. The use of temtum would also give the users additional benefits such as increased anonymity while using the application.

e-Commerce payment gateway

The e-commerce market

By 2021 the e-commerce industry will equate to $4.8tn in sales[16], with every transaction currently accompanied with a transaction fee, either from a payment gateway such as PayPal or Sage, from bank and credit card providers such as Visa and Mastercard, or from a cryptocurrency such as Bitcoin or Ether.

Borderless transactions in e-commerce are significantly increasing each year[17] as retailers target new and emerging markets, whereby currency conversion rates, on top of multiple payment processor transaction fees, are not only overcomplicating financial planning for merchandisers but also directly impacting revenues, running into $millions per year for some major retailers.

The returns dilemma

2018 data shows that 20% of online purchases are returned[18]. This is particularly prevalent in apparel and fashion retail, where consumers are taking advantage of competitive returns policies to have their own at home fitting service. With the opportunity to return items now potentially increasing conversions by up to 72%[19] and original transaction fees not returned to the merchant, e-commerce payment processing is ripe for disruption by instant, feeless cryptocurrencies.

For example, using the figures above for a leading UK payment gateway's lowest transaction fee of 0.75%[20], 20% returns on a $4.8T industry in 2020, equates to $960bn with up to $720m lost in transaction fees on returned items where the retailer is left with no sale revenue.

temtum as a payment gateway

There are currently two methods of accepting temtum for e-commerce businesses:

1. **Full temtum e-commerce** – An online store which accepts temtum for goods – the store has their own wallet for payment and existing e-commerce infrastructure.

2. **Online stores accepting temtum** - This works like a regular store – with a 'pay with temtum' button – but this is automatically converted to fiat via an exchange, so the store never holds or even receives TEM, only fiat.

To ensure the adoption of TEM as a viable e-commerce payment solution, we've developed a Shopify payment plugin, along with a 'temtum pay' process, featuring a quick-buy button, much like those from Amazon and PayPal. This plugin will also be available via our API for custom payment solutions.

This will help us to achieve our goal of mass adoption of the currency and it can be deployed on day one, since we have already developed these features.

[16] https://www.shopify.com/enterprise/global-ecommerce-statistics

[17] https://www.shopify.com/enterprise/global-ecommerce-statistics

[18] https://www.shopify.com/enterprise/ecommerce-returns

[19] https://www.shopify.com/enterprise/ecommerce-returns

[20] *https://www.quba.co.uk/insights/blog/may-2018/guide-our-cost-calculator-for-worldpay-sage-pay*

The buying process

- **A unique address will be created for each basket for the merchant and linked with the details of consumers.**

- **A consumer will send TEM directly to this address, as part of an instant payment transfer, and receive the goods from the merchant.**

For consumers this will be a standard TEM transaction and they would not be required to do anything differently than they are used to in order to buy with their temtum.

The benefits for the retailer to implement TEM transactions include:

- **Faster confirmation time – TEM confirmed in their account in under 12 seconds, trackable on our block explorer**

- **No transaction fees**

- **No lost transaction fees on returns**

- **New audience segmentation**

- **No bank charges**

Cryptocurrencies hold the key to significant savings for merchants but they require greater adoption of payment coins in order for their benefits to be realized in full. While payment gateways sit between consumer and merchant, transaction costs will always exist.

Competitor Analysis

temtum
Cryptocurrency. Evolved.

Introduction

temtum is launching in an increasingly congested cryptocurrency marketplace. However, we believe that our product offers unique advantages and, as mentioned above, represents a step-change in the evolution of blockchain. Our ambition to be the first cryptocurrency to achieve mass adoption is not matched by any other credible cryptocurrency that has been developed, deployed and tested. This section represents a brief review of some of the cryptocurrencies that we regard as being key competitors.

Commentators and regulators[21] have divided cryptocurrencies into three main categories:

- **Payment coin (or exchange coin) – a means of payment or value transfer**
- **Utility token – that provide access to a service**
- **Security token (or asset coin) – that represent rights in or to assets or businesses**

Whilst it is possible to see significant value in a payment coin (as a direct alternative currency, like Bitcoin)[22], and in a security coin (due to the rights in or to underlying assets or businesses), many cryptocurrencies are instead issued as utility tokens.

Utility tokens claim to give holders access to rights to use services associated with the issuer platform (often platforms which are not yet developed) as a form of voucher or club membership. They are often intended to disrupt a particular industry or business model. Whilst the services – once the issuer platform has been developed – may have value, this value will be more limited to a particular industry or a fraction of the population that values those types of services.

In many jurisdictions, security coins are likely to be subject to more restrictive regulation on the ability of the coin issuer to sell and distribute them internationally than payment coins or utility coins, as they are likely to be governed by differing national regulatory requirements on the offer and sale of securities such as shares, bonds or collective investment schemes.

We do not believe that any coin other than a global payment coin could realistically constitute a competitor for temtum. The current leading cryptocurrency, Bitcoin, has a range of flaws that limit its ability to act as an effective medium of exchange – flaws which have been addressed in the design of temtum.

Bitcoin

temtum in many ways represents an effort to take many of the admirable and pioneering blockchain ideas behind Bitcoin and make them fit-for-purpose in terms of being secure, scalable and available to a mass-market of users. That is why we view temtum as a step-change in the evolution of blockchain. It is clear that Bitcoin cannot hope to achieve acceptance as a mainstream payment coin. The graphs below show the current state of Bitcoin which clearly demonstrate a network that is at capacity and no longer able to process all transactions. We believe that Bitcoin:

- **is at capacity;**
- **has a backlog oftransactions;**
- **uses too much RAM;**
- **uses too much internet bandwidth;**
- **uses too much storage space; and**
- **cannot scale and maintain security because of its reliance on proof-of-work.**

[21] For example, FINMA in Switzerland https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

[22] For example, An (Institutional) Investors Take on Cryptoassets https://medium.com/john-pfeffer/an-institutional-investors-take-on-cryptoassets-690421158904

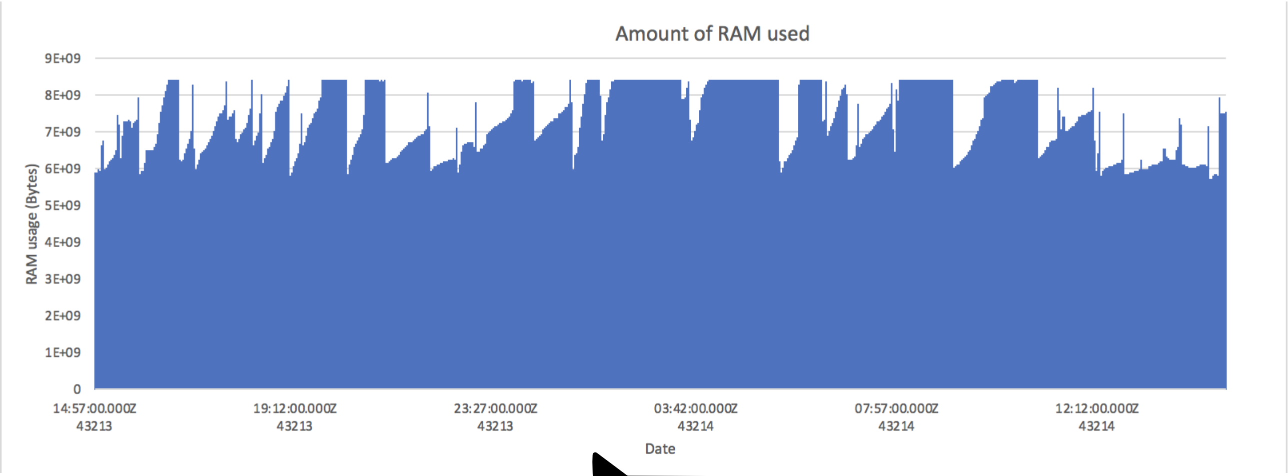


Fig 23: Amount of RAM required to run a blockchain in Bitcoin

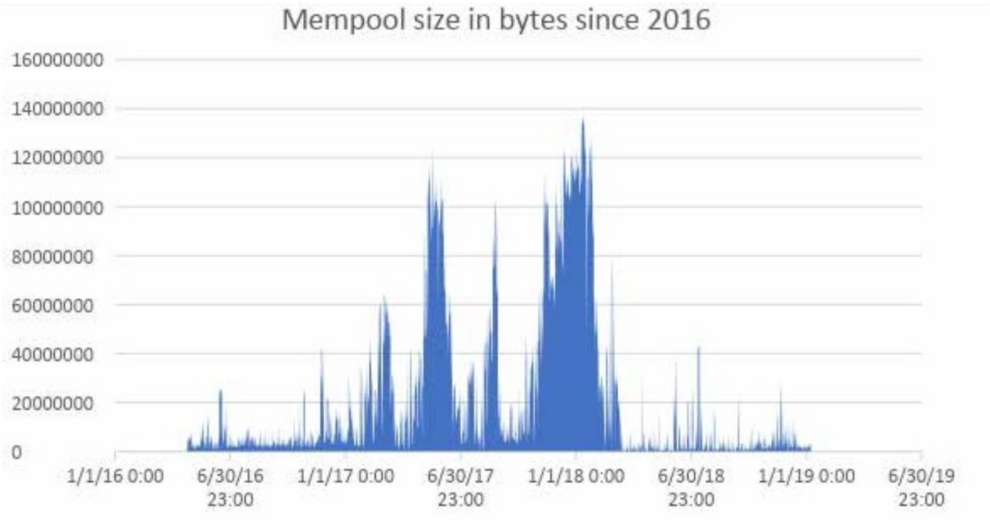


Fig 24: Mempool size in Bitcoin

Size of the mempool (in bytes) in Bitcoin (this is the backlog of transactions which cannot be included into blocks due to the block size limit)

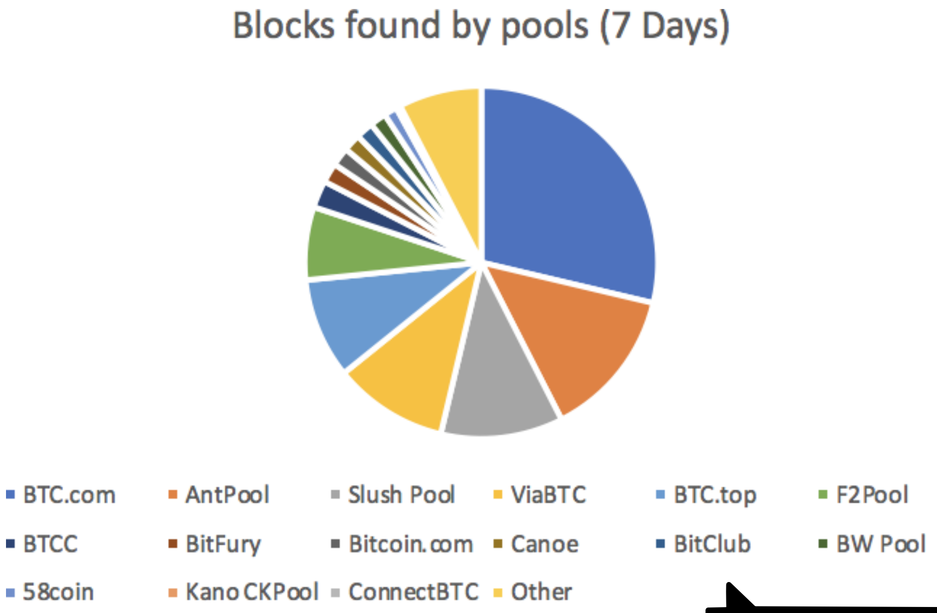


Fig 25: Mining pools for Bitcoin

Bitcoin is centralized. Mining pools are responsible for the majority of blocks found, and just three control over 51% of the network – this is not a decentralised network

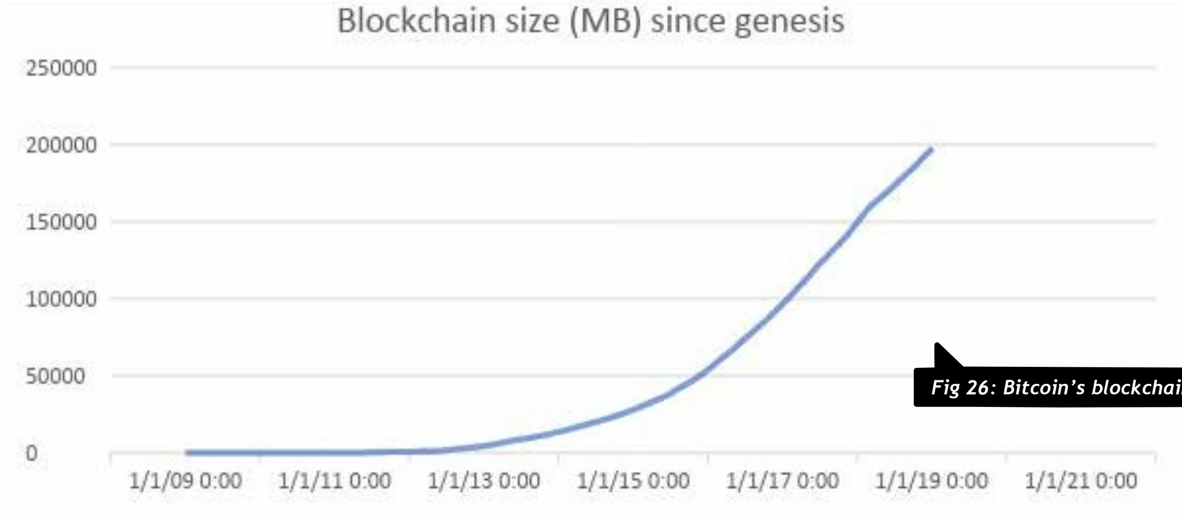


Fig 26: Bitcoin's blockchain size

Bitcoin's blockchain size. The blockchain is always growing and all nodes must download the full chain.

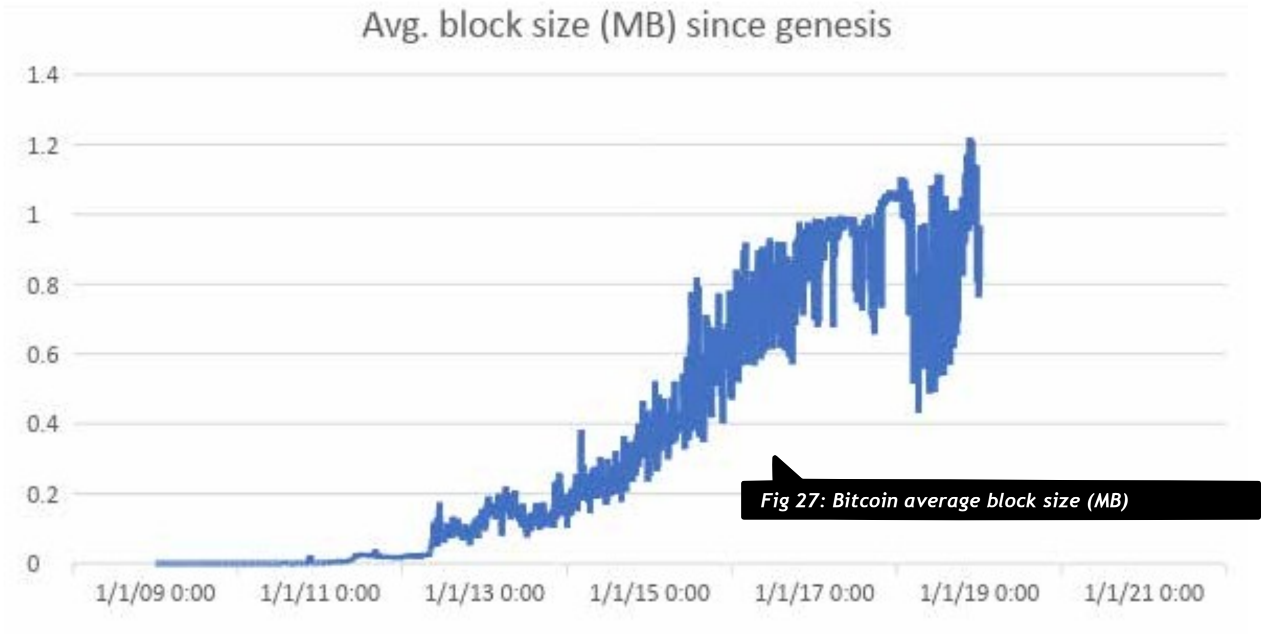


Fig 27: Bitcoin average block size (MB)

Total bandwidth received used since restart

Shows that block sizes are increasing until the block size limit was hit.

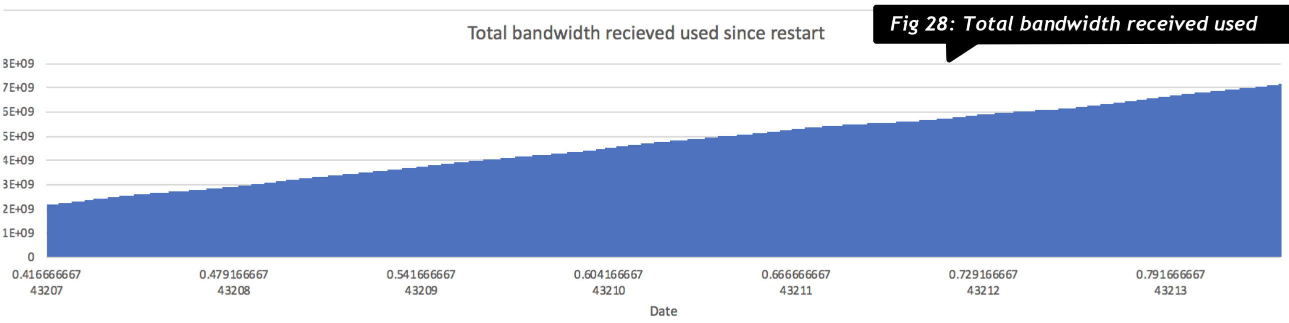


Fig 28: Total bandwidth received used

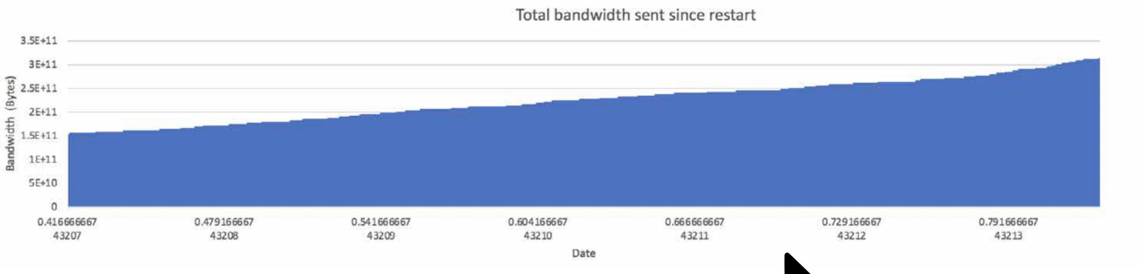


Fig 29: Total bandwidth sent

The total amount of network bandwidth used by a basic blockchain node over a period of four days (Bitcoin).

We are not aware of any blockchain networks that we believe are sufficiently advanced to be direct competitors for temtum.

We've looked below at some other (non-blockchain) software solutions that are designed to offer payment system solutions.

Nano

Nano is a digital currency system designed for speed and efficiency that uses a block-lattice structure to distribute a ledger across each node using a directed acyclic graph (DAG) architecture. Individual accounts track their own balance and transaction history to build an asynchronous network. Exchanging Nano is a two-step process where a sender must initiate a send transaction, while the receiver adds a receive transaction.

Despite having certain features of a traditional blockchain, such as a delegated proof-of-stake consensus algorithm, Nano is not a blockchain network. It does not use mining and does not contain a full history of transactions on the chain every time it processes a transaction – only balances.

Analysis: The two-step process introduces an inefficiency as it requires both users to go online simultaneously. We do not believe that Nano currently has widespread usage, or links to traditional banking infrastructure.

Hedera

Hedera Hashgraph is based on distributed ledger technology like blockchain that works on a graph-like structure where all the nodes communicate their information to each other, and their communication is reported by building a graph of connections.

All the information or data is stored in events. It relies on 'gossip about gossip' and 'virtual voting' mechanisms to bring consensus to the network.

It is not a blockchain and no one node has the entire history stored locally as shown below:

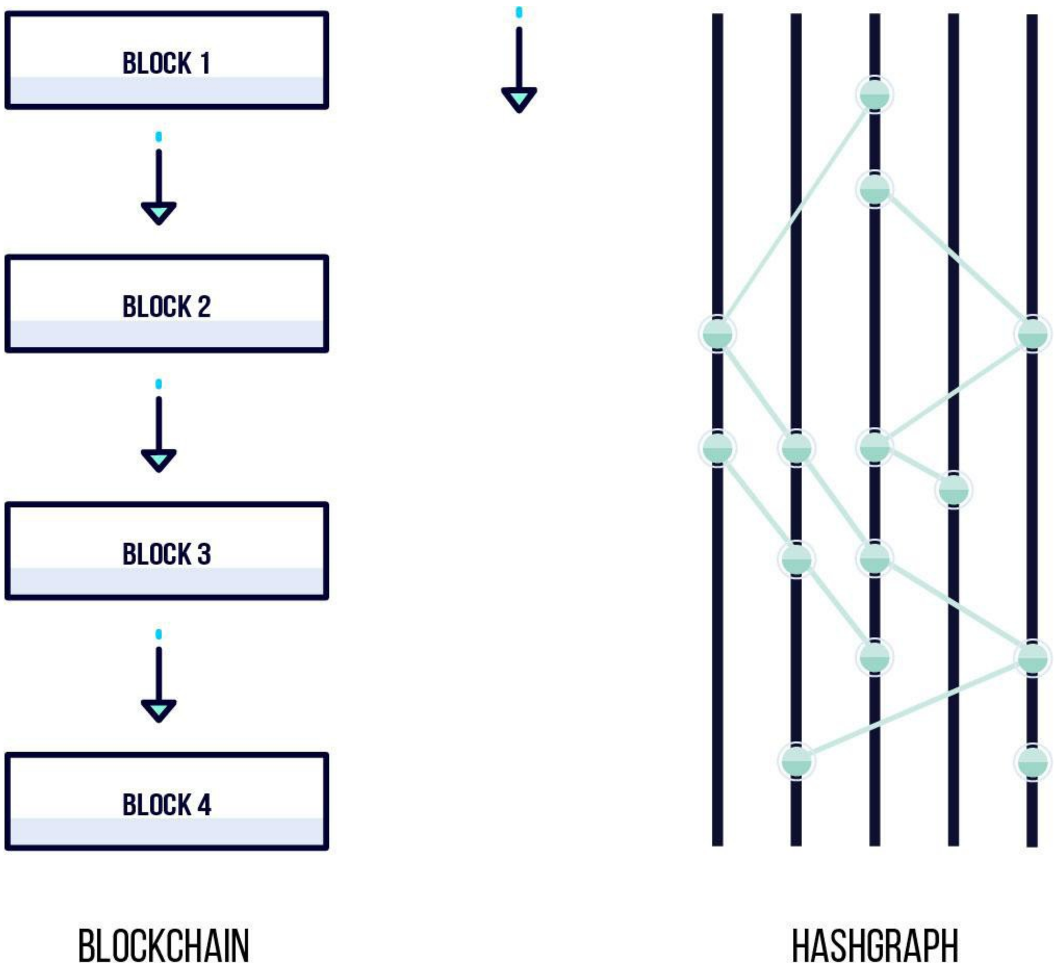


Fig 30: Network participants

This is only secure if up to a third of the nodes are malicious. This is substantially lower than the 50% of malicious nodes Bitcoin can handle, and significantly lower than the Temporal Blockchain as well. In our view this shows an attack against Hedera could be conducted cheaply and fast, since any node would be able to join the network without any reputation system ensuring honesty.

Their use of the gossip protocol also shows a lack of network optimization as shown in Bitcoin, where the gossip protocol is responsible for a packet being duplicated more than 18 times.

As more transactions per second are sent through the network, a significant amount of network bandwidth will be used by the repetition of packets because of the gossip protocol, limiting the real world number of transactions able to be confirmed by the network.

Analysis: This is a very interesting technology which aims to solve some fundamental issues with Bitcoin and traditional blockchain networks, but it faces security and scalability issues when the network goes from private to public.

Other noteworthy currencies include:

Ripple

Ripple was originally released in 2012 as a revised iteration of Ripple pay. It is not a blockchain network. Instead, Ripple is a real-time gross settlement system (RTGS), currency exchange and remittance network. Banks are able to use the Ripple software to transfer money between different currencies. This is typically accomplished using SWIFT, a system that is cumbersome and relies on the banks having separate accounts in every country they work in. Ripple states that it has signed up more than one hundred banks.

Ripple uses a common shared ledger that is managed by a network of independently validating servers, using a hash tree to summarize data into a single value that is compared across the servers using a consensus process to ensure integrity. Ripple also maintains a trusted Unique Node List (UNL) that is meant to protect against potentially malicious or insecure validating servers. Ripple does not rely on the energy and computing-intensive proof-of-work used by Bitcoin.

Analysis: As the purpose of the Ripple platform is a bank-to-bank system to transfer currencies around the world rapidly, we do not believe that the Ripple token (XRP) is integral to the operation of the system. In addition, the system is for bank-to-bank transfers, so it does not create a direct payment rail for consumer and merchants.

We do not see Ripple as a direct competitor to temtum.

Stellar

Stellar is a system that settles financial transactions through a peer-to-peer network. It is not a blockchain network. It aims to compete with other rapid settlement infrastructure platforms such as Ripple. In fact, its creator is an ex-Ripple executive and the blockchain of Stellar is itself a hard fork of the Ripple chain. It focuses on penetrating the financial sector and bringing banking services to the unbanked. Stellar is partnered with IBM as part of its Hyperledger Fabric Project. It also partnered with American Express on an international payments channel.

The system uses a token, lumens (XLM), which is used to pay transaction fees (a fee of 0.00001 XLM is required for transactions on the Stellar network). Instead of mining, XLM are automatically generated at an inflation rate of 1 percent of the total supply every year. This inflation pool is distributed among account holders based on the percentage of XLM held. Voting rights on the network are also determined by the amount of XLM held. It is not necessary for every Stellar node to validate every transaction. Instead, each node chooses a set of trustworthy nodes for its group.

Analysis: As with Ripple, we do not believe the XLM token is the core focus of the system.

We do not see Stellar as a direct competitor to temtum.

Network Integration

temtum

Cryptocurrency. Evolved.

Introduction

In order to successfully launch the temtum network, we have conducted what we believe is the largest amount of network and application security testing – verified by multiple rounds of pentesting via a Crest accredited agency – by a cryptocurrency before mainnet launch. The temtum network has been deployed as a test net for over six months as of January 2019, and has not suffered any downtime, intrusion or other issue which caused any malfunction of the blockchain.

The logistical real-world integration of the temtum network is a critical element of our overall value proposition and we have spent significant effort on seeking to ensure that the relevant details have been considered and tested.

Deployed network and applications

We have developed and deployed:

- A fully operational mainnet hosted on numerous servers in multiple countries which has been proved to far exceed our initial engineering specification for transaction throughput.
- Fully functioning and deployed temtum Network API.
- Fully developed applications for web, Android and iOS devices tested both within and between various countries globally, including but not limited to, Belarus, Ecuador, UK, Belgium, USA, Zimbabwe and South Africa.
- An SMS-based system to enable temtum transactions on any type of mobile phone including feature phones.
- Working nodes on a range of IoT devices including an i8 car and a smart watch.

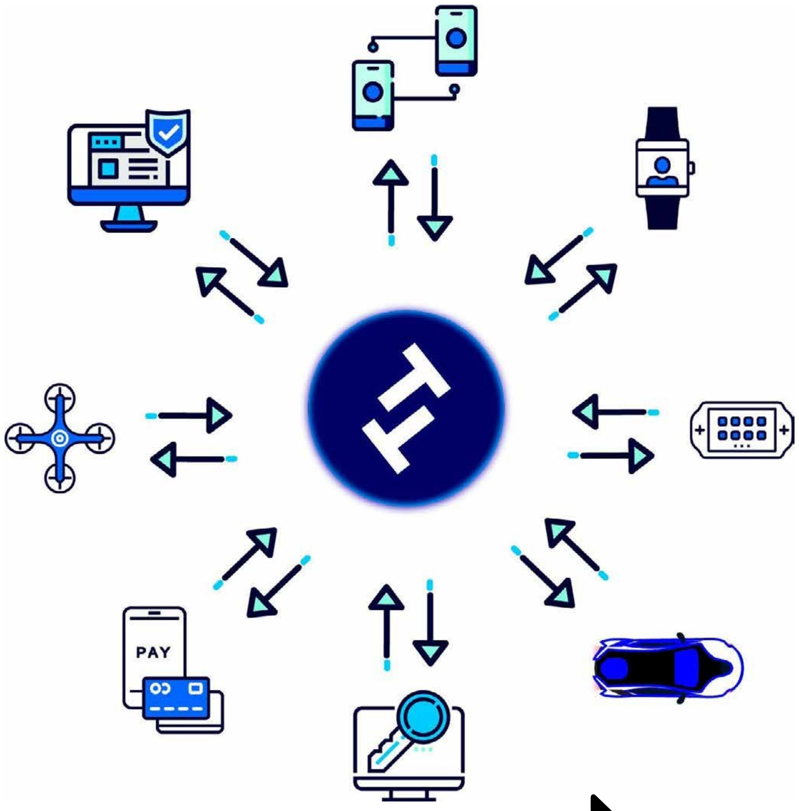


Fig 31: Network participants

The mainnet will be launched when the genesis block is created at the point of any TEM distribution. We have proven that the network we've created has exceeded the original technical specifications we worked towards.

The network is hosted on more than 100 servers globally, with data centers used but not limited to:

- Europe > Amsterdam (AM)
- Asia > Singapore (SP)
- Asia > India, Bangalore (IN)
- Western Europe > London (UK)
- North America > Canada (CA)
- Central Europe > Frankfurt (DE)

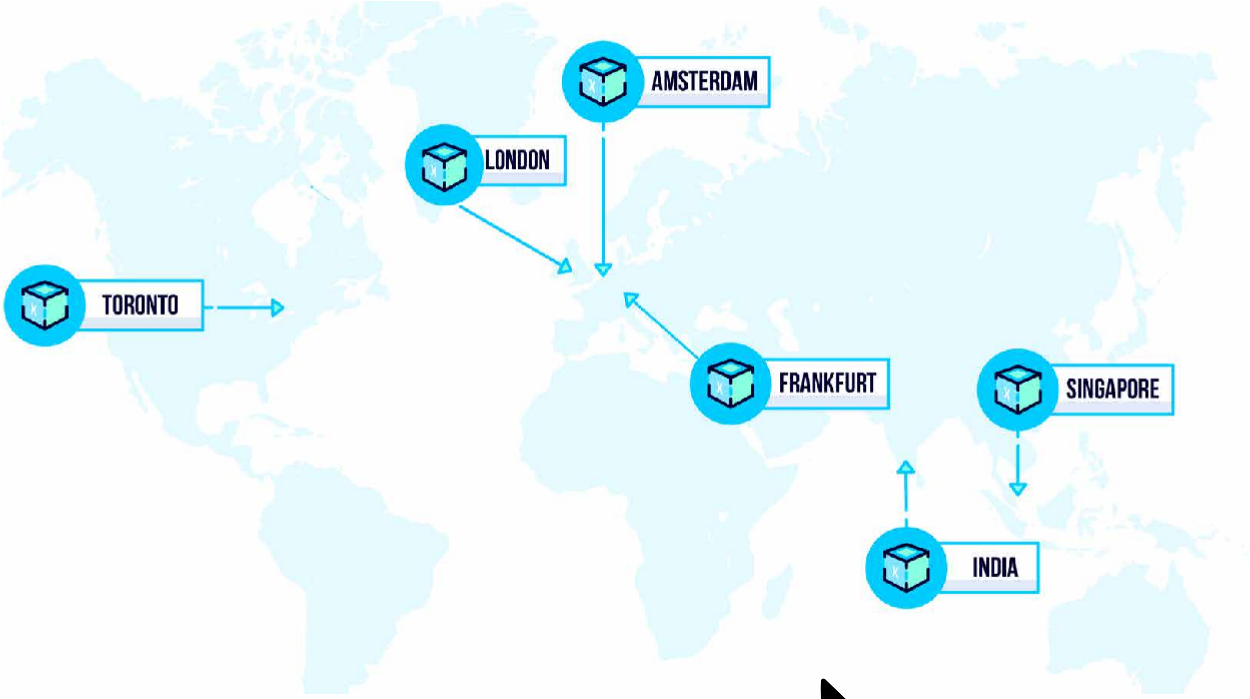


Fig 32: Current server map

Each node is also snapshotted at regular intervals and all blockchain data is backed up offline, as well as all logs of the wallet and apps.

temtum API

Our API allows developers to send transactions directly to the temtum network and create new addresses for these transactions if needed. As outlined in detail in our road map, this will allow banks and other financial organizations to make instant money transfers without any commission or delays and will open up new opportunities for existing financial institutions.

The temtum API provides the foundations for exciting development projects where technology provides no barriers whatsoever for the implementation of cryptocurrencies for mass use.

To promote adoption of temtum and allow developers to interact with the network, an API has been created with detailed and always evolving documentation, available online.

In addition to the API – Our GitHub contains open source code to temtum-developed products such as the wallet, the block explorer, API and blackjack gaming app, amongst others. This will always be added to and maintained, while the community are actively encouraged to fork and develop upon the codebase.

Currently the API provides the ability to:

Auth

- Change token and refresh token of the logged user (an active token is mandatory)
- Check if reset password token is valid
- Check if the access token is still valid
- Check if username and email are available
- Deactivate user when he/she is trying to delete(close) their account
- Login to the account
- Logout the user (provide token in Beaver header)
- Resend SMS code at sign-up
- Send a confirmation email to the user when he/she forgets their password
- Send a confirmation email to the user's new email when he/she forgets their password
- Sign up to the wallet
- Verify SMS code when signing up

Countries

- Get available countries

Device

- Delete user's device that was used previously
- Get user's devices
- Verify user's device

FAQ

- Get FAQ data

History

- Get user's login history

User

- Add push notifications client token
- Change google 2FA permissions

- Change the user's email
- Change the user's name
- Change the user's pin
- Change the username
- Confirm the email change
- Confirm a new email
- Create a transaction
- Disable user's pin
- Find username (at least 3 symbols of username are required)
- Get address (public key) of the user (provide token in Bearer header)
- Get the balance of the user
- Get the encrypted private key
- Get the user info
- Get the user's transactions history
- Resend confirmation email
- Send encrypted private key to email
- Send transaction
- Set smart authentication protection status
- Set user's pin
- Verify user's pin

UserIP

- Delete user's IP that was used for logging previously
- Get user's IPs
- Resend confirmation email
- Verify user's IP

Wallet system

The temtum wallet works in the same way as a bank account in two fundamental ways – it is both a repository for currencies and a mechanism for completing transactions. Each wallet uses temtum technology to make transactions with other wallets on the network. But it is also different to a conventional bank account in other ways, such as:

- **The wallet can be identified with only a username and/or wallet-address.**
- **Transaction speed: transactions will be confirmed within 12 seconds instead of waiting for days.**
- **Every transaction is confirmed by a decentralised network.**
- **temtum transactions have been tested using the web application, mobile applications, drone, watch, raspberry Pi and even a car.**

The temtum wallet is a cryptocurrency wallet where users can manage their TEM. We have combined all the necessary elements including security, simplicity, and easy access. The temtum website has full details of all the applications and examples of how to use the features of each application.

temtum keyboard

This unique smartphone keyboard allows the user to access the benefits of the temtum application in a seamless way and can be used from any mobile messaging application. It means that users can simply click on a custom temtum button and, without opening the temtum app, temtum coins (TEM) can be sent from one account to another.

The keyboard is installed as a customized keyboard service as part of the temtum application. This enables sharing of the core functionality and the stored user credentials using the most secure standards for mobile apps. The user can access the temtum transfer functionality very simply from any application.

Both these features – the temtum application and the temtum keyboard – use the same temtum API capabilities and apply the same security standards. This design ensures data integrity between transactions either for the temtum mobile application and the temtum keyboard.

The model to connect to the temtum API from mobile and keyboard application is as follows:

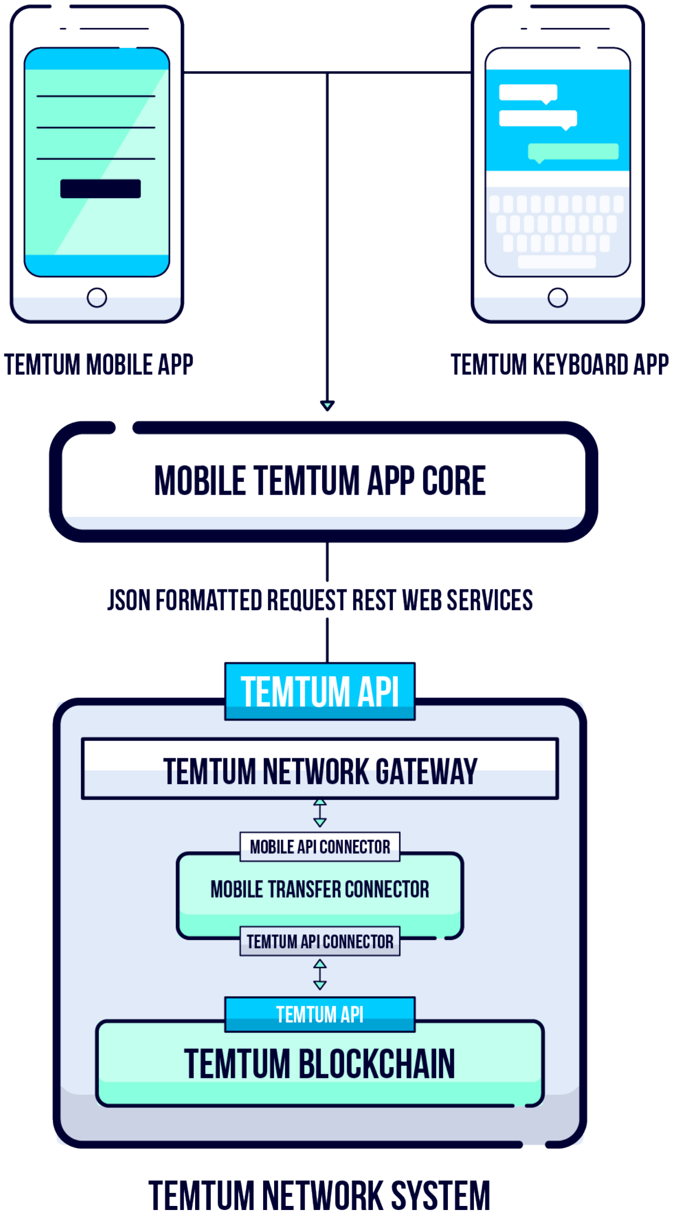


Fig 33: Mobile apps API integration

SMS payment transfers

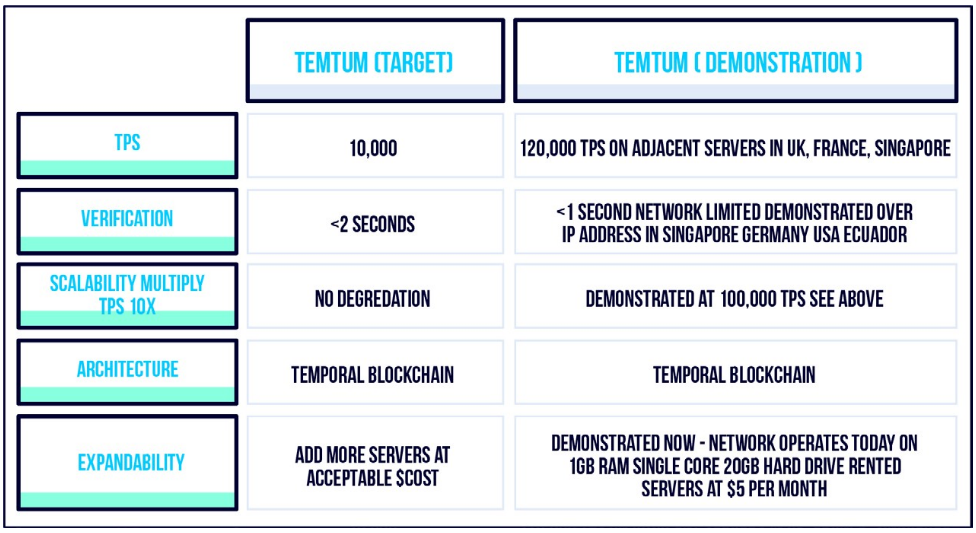
We have developed an SMS-based system to allow any user to send temtum to any other user by sending an SMS message.

The SMS system does not require users to download an app, and there are no requirements for accounts or passwords. If the user has a device that can send an SMS text message, then they are able to use temtum. Similarly, the recipient needs neither an app nor a wallet to receive funds. This makes it suitable for non-smartphones and is targeted at countries with a high penetration rate of such devices, the use of which is driven by unpredictable electrical power and intermittent, or less widely available, high speed internet.

The SMS system allows for instant transfers. Transactions are immediately settled directly on the Temporal Blockchain and funds are never held by a third-party.

Network performance

Transactions per second (TPS)



	TEMTUM (TARGET)	TEMTUM (DEMONSTRATION)
TPS	10,000	120,000 TPS ON ADJACENT SERVERS IN UK, FRANCE, SINGAPORE
VERIFICATION	<2 SECONDS	<1 SECOND NETWORK LIMITED DEMONSTRATED OVER IP ADDRESS IN SINGAPORE GERMANY USA ECUADOR
SCALABILITY MULTIPLY TPS 10X	NO DEGREDATION	DEMONSTRATED AT 100,000 TPS SEE ABOVE
ARCHITECTURE	TEMPORAL BLOCKCHAIN	TEMPORAL BLOCKCHAIN
EXPANDABILITY	ADD MORE SERVERS AT ACCEPTABLE $COST	DEMONSTRATED NOW - NETWORK OPERATES TODAY ON 1GB RAM SINGLE CORE 20GB HARD DRIVE RENTED SERVERS AT $5 PER MONTH

Fig 34: temtum performance targets

Using our algorithm, a mainstream CPU such as the Intel 8 Core i7 7820X can theoretically perform 20,000 transactions per second. Future delegation implementation in the temtum network as described in the roadmap section of this document will allow six relatively common home machines to support 100,000 transactions per second.

temtum has no theoretical limit on transaction throughput – our process is only limited by the hardware and network bandwidth available.

The temtum network requires a bandwidth level of just 13.3 megabits/second in order to compete with existing payment gateway networks (assuming an average rate of 2,000 transactions per second at an average transaction size of 874 bytes). This level of bandwidth is common for standard residential connections around the world today – a 2018 Ofcom study[23], for example, demonstrates an average home broadband speed of 46.2Mbps in the United Kingdom.

Current blockchain networks are further restricted in transaction throughput by the time it takes to validate a signature. The Temporal algorithm dramatically reduces the amount of data that must be analyzed in order to validate a signature compared to proof-of-work blockchain networks such as Bitcoin.

The delegation of roles is not yet fully implemented in the temtum network but, when it is, it will allow our network to scale by using agile load handling, making it possible to add resources to deliver performance increases as needed. This functionality is not possible with the current generation of blockchain networks.

[23] Ofcom Fixed Home Broadband Speeds Report 2018: https://www.ofcom.org.uk/_data/assets/pdf_file/0027/113796/home-broadband-2017.pdf

An energy-efficient network

The temtum network is extremely energy-efficient when compared to other blockchain networks. The temtum Consensus Algorithm, combined with Temporal Blockchain technology, is able to confirm all transactions with one machine at a time. We estimate that the overall Bitcoin network is 16,573,693 times more expensive than the temtum network based on energy costs alone, assuming both networks are operating at the same size.

A temtum network node operating on a standard home machine, utilizing a single core of an Intel i7 2.60 GHz and 16GB of RAM with an estimated energy consumption of 200 watts is able to confirm all transactions demanded by every network participant. International Energy Agency data demonstrates that worldwide electricity prices do not exceed $0.36 per kWh[24] as of May 2018.

Assuming the highest international electricity price, the continuous 24/7 operation of the temtum network across 1752 kilowatt-hours in a single year would cost just $631.

In comparison, the proof-of-work consensus mechanism used in current-generation blockchain networks is computationally intensive. The Bitcoin blockchain, which is currently the largest proof-of-work blockchain network, uses a vast amount of electricity. As of May 16, 2018, the Bitcoin network was estimated to consume at least 2.55 gigawatts of electricity.

As of September 29, 2018, the Bitcoin network consumed 73.12 TWh of electricity, accounting for 0.33% of the of the world's electricity consumption[25] – as much as is consumed by the entire country of Austria. Bitcoin mining is currently consuming more electricity than 159 countries worldwide[26].

As of January 2019, Bitcoin consumes 46.55 tWh of electricity.

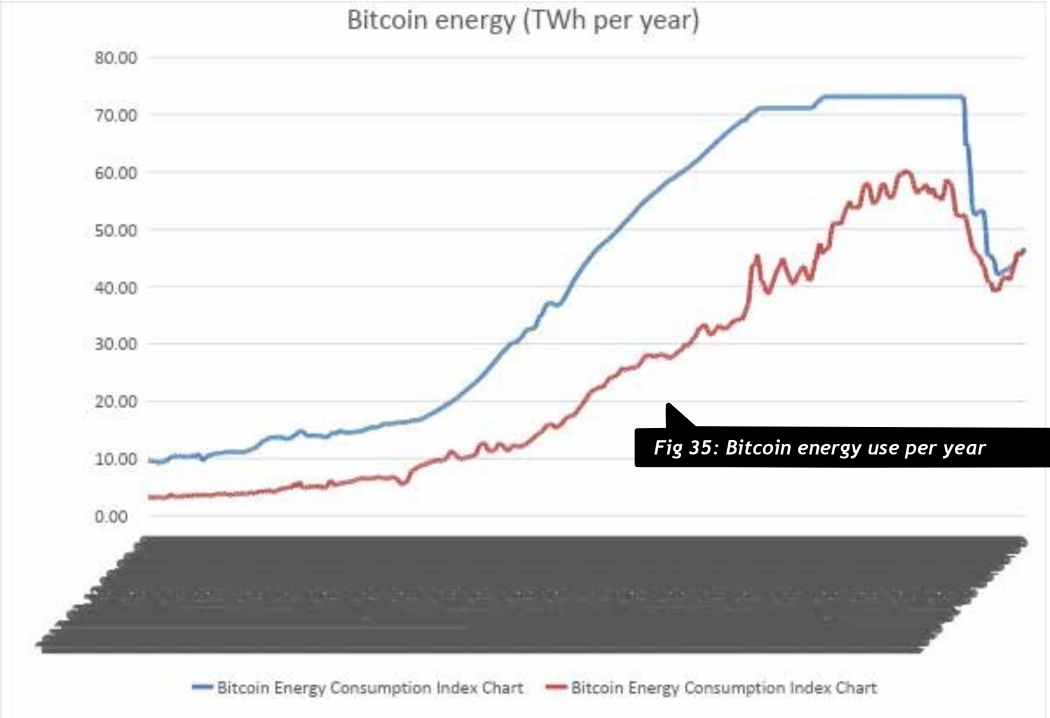


Fig 35: Bitcoin energy use per year

[24] World Energy Prices: An Overview: https://www.iea.org/publications/freepublications/publication/WorldEnergyPrices2018Overview.pdf

[25] https://digiconomist.net/bitcoin-energy-consumption

[26] https://www.eia.gov/beta/international/data/browser/#/?c=4100000002000060000000000000g000200000000000000001&vs=INTL.44-1-AFRC-QBTU.A&cy=2016&vo=0&v=H&end=2017

The recent drop in energy use is due to the drop in the price of Bitcoin – as the Bitcoin price decreases it becomes less economically attractive to invest in mining operations. And when Bitcoin's price falls, marginal miners drop out as the cost of mining Bitcoins starts to exceed the rewards. However, this also creates a security risk. As the mining pool shrinks, there is a higher likelihood of attempts to seize control of the pool with a 51% attack. According to a January 2019 report from the Bank of International Settlements (BIS), ‘the [Bitcoin] system cannot generate transaction fees in line with the goal of guaranteeing payment security. Either the system works below capacity and users’ incentives to set transaction fees are very low, or the system becomes congested.’[27] But for the temtum network there is absolutely no such correlation. In short, the security of the temtum network is not related to the price of temtum coins in any way whatsoever.

Data of Bitcoin energy usage as of January 2019

Description	Value
Bitcoin's current estimated annual electricity consumption* (TWh)	46.56
Bitcoin's current minimum annual electricity consumption** (TWh)	46.56
Annualized global mining revenues	$2,640,302,394
Annualized estimated global mining cost	$2,243,741,891
Current cost percentage	84.98%
Country closest to Bitcoin in terms of electricity consumption	Iraq
Estimated electricity used over the previous day (KWh)	127,561,205
Implied Watts per GH/s	0.115
Total Network Hash rate in PH/s (1,000,000 GH/s)	46,101
Electricity consumed per transaction (KWh)	471
Number of U.S. households that could be powered by Bitcoin	4,311,096
Number of U.S. households powered for 1 day by the electricity consumed for a single transaction	15.91
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	0.21%
Annual carbon footprint (kt of CO2)	22,814
Carbon footprint per transaction (kg of CO2)	230.61

Fig 36: Bitcoin use data Jan 2019

The energy consumption of the Bitcoin network is increasing at a rapid rate. Bitcoin mining energy consumption increased by 29.98% during the month of September 2018[28].

Transaction costs

We believe that temtum network transactions are 36,633,497 times cheaper than Bitcoin transactions, based on the below projections. The economic impact of the consensus method used to operate the Bitcoin network absorbs an estimated cost of $3.6 billion annually.

[27] Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies', January 2019: https://www.bis.org/publ/work765.htm

[28] https://www.blockchain.com/en/charts/hash-rate

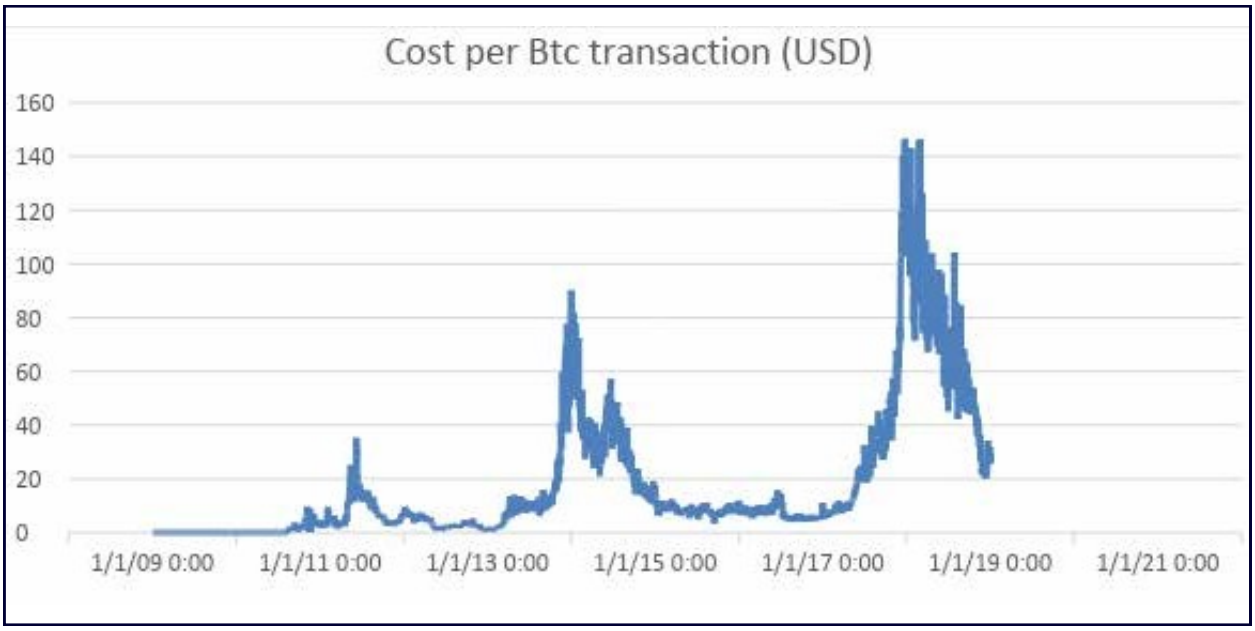


Fig 37: Cost per Bitcoin transaction

Operating at the same size as the Bitcoin network and executing the same amount of transactions, the temtum network reduces the cost of an individual transaction to $0.0000029 by eliminating miner fees and reducing energy consumption.

The Bitcoin transaction cost is dependent on network load – higher load = high fees, with temtum network load does not impact cost of transaction – there is never any network fee.

CREST - approved security testing

The security of the temtum network has been independently tested on a theoretical and deployment level by a UK CREST-accredited information security firm – BSI group.

The Council for Registered Ethical Security Testers (CREST) are a non-profit accreditation and certification body that represents the technical information security industry. CREST provides internationally recognized accreditation for organizations and individuals providing penetration testing, cyber incident response and threat intelligence services, endorsed by the UK GCHQ signals intelligence and information assuranceorganization.

The BSI Group, also known as the British Standards Institution (BSI), is the national standards body of the United Kingdom. BSI produces technical standards on a wide range of products and services, and also supplies certification and standards-related services to businesses.

They have been chosen due to their knowledge and experience in testing cryptographic products, as well as their high reputation for in-depth and detailed security testing work.

BSI have successfully completed five rounds of security testing which first began on 12th July 2018. The full reports can be found under the 'Reports' section of the temtum website.

As the project progressed, the scope of the testing changed, from ensuring the underlying technology, cryptographic protocols and implementation are secure and are behaving as described, to conducting a more mainstream penetration test and security review of the web application (wallet), Android and iOS applications.

One round of testing was focused on ensuring correct implementation of both the theoretical underpinnings and implemented code elements of the Temporal Blockchain. The next two rounds of testing focused on the security of the network and front-end GUI (temtum wallet). Finally the Android and iOS wallet applications were tested.

Summary of testing undertaken 12th July 2018

BSI Cybersecurity and Information Resilience were engaged by Dragon InfoSec to perform a security assessment against their custom blockchain implementation. Testing was undertaken remotely between the 5th and 12th of July 2018.

The scope of the engagement was as follows:

» **Perform a double-spend**

» **Inject a malicious transaction into the blockchain**

» **Generate the private key from its associated public key**

» **Delete a transaction from the blockchain**

» **Assess the public API**

» **Assess the cryptographic routines used for address generation**

» **Assess the security of the NIST time beaconing • Assess the implementation of the blockchain storage**

While certain minor issues were identified, which were due to the early stage of development of the network, the implementation of code and the theoretical basis of the unique Temporal Blockchain were successfully validated.

Summary of testing undertaken 21st September 2018

The next test was to perform a web application test against the temtum wallet application. Testing was undertaken remotely between the 17th and 18th September 2018.

The scope of the engagement was to:

» **Perform security testing of the web application.**

» **Ensure that users' private keys could not be exposed.**

» **Ensure that transactions can only be performed with authorized accounts and valid balances.**

Whilst BSI did detect some minor issues, which were readily addressed, the testing once again assured the security of the underlying technology with no security issues or vulnerabilities detected, but the issues detected related to the implementation of the web app (wallet).

Summary of testing undertaken 6th December 2018

The third round of testing was to perform a web application penetration test against the temtum Wallet web application. Testing was undertaken remotely on November 26th and 27th 2018.

The scope of the engagement was to:

» **perform a retest of the application; and**

» **test new functionality including the Bitcoin to temtum conversion and 2FA.**

This testing was a follow-on from the previous round of testing, aiming to:

- **confirm that all previous security issues have been fixed; and**
- **test of additional features implemented since the previous round of testing.**

While BSI did detect several low-level issues, these were quickly resolved during testing and this test provided a positive result for the web application, demonstrating the underlying technology is secure from any major security issues or vulnerabilities.

Summary of testing undertaken 21th December 2018 – Android wallet

BSI Cybersecurity and Information Resilience were engaged by Dragon InfoSec to perform a web application test against the temtum Android wallet. Testing was undertaken between the 11th and 13th December 2018 remotely.

The scope of the engagement was as follows:

Android Application Test:

- **temtum Android Wallet**

Testing was focused on the implementation of the two-factor authentication feature.

Database configuration Review:

- **Wallet SQLite Database**

Server Build Review:

- **CI-SERVER**

While BSI did detect several low-level issues, these were quickly resolved during testing and this test provided a positive result which established that the web application, along with the underlying technology, is secure from any major security issues or vulnerabilities.

iOS testing is currently being conducted and results will be published once testing is completed, although early indications show no serious security issues or vulnerabilities.

This section outlines our intended strategy for implementing the key network technology integration required for the successful running, and mainstream adoption, of the temtum network.

Technology Roadmap

temtum

Cryptocurrency. **Evolved.**

Application and functionality development

IoT and mobility implementations

Phase 1: BMW i8

To demonstrate the technical capabilities of the temtum network – and how few resources a node is required to have in order to participate in the blockchain – we deployed custom code on the head unit (HU) of a BMW i8 as part of a mobility focused project. This allowed the car to function as a fully working node, capable of confirming transactions as the car was driven. The loading of the code into the car did not have any impact on its functionality and was able to run in the background.

Even though the computing power in the i8 is significantly less than traditional computers, it consistently demonstrated the ability to confirm 500 TPS.

We believe this is a world-first where a car has been able to act as a full node without the requirement of additional hardware.

Further developments of the mobility project have focused on two main areas:

1. The creation of a mesh network using cars as nodes, facilitating node-to-node communication; and
2. How this can be integrated into the wider temtum network.

Two test cars, a BMW 220i, and the showcase BMW i8 have been used during testing. As in the previous development cycle, we did not add any additional hardware and only the software on the iDrive systems were modified. We discovered that the BMW 220i, while a significantly less advanced in terms of digital systems than the i8, was still able to fully participate and achieve the same level of performance as a full node (able to store the Temporal Blockchain and confirm transactions when required) as the flagship i8.

Phase 2: Car-to-car

After demonstrating that an entry-level BMW is fully capable of participating in the temtum network as a node, we also achieved a mesh network between cars. This allowed the BMW 220i to have its own mobile network connection disabled, leaving it without internet access and instead receive data directly from the i8.

Receiving data from the i8 to the 220i directly, where Temporal and all transactions are also using cryptography, would not present an attack vector. The ability to communicate with vehicles that do not have an active internet connection increases the opportunity for older cars to participate in the network, while removing any mobile data charges and reducing costs for network participation.

Sideloading our application into the existing entertainment system of the older model BMW showed no performance degradation to the driver. Testing is under way to apply this theory to more car brands, including a 2018 Renault Megane, which will allow for direct cross-platform (i.e. from brand A to brand B) communication.

More than half-a-million BMW vehicles were registered in the UK from January 2014 to January 2017, with each vehicle more than capable of participating in and supporting the temtum network. With network scale increasing attack costs, participation via existing mobility infrastructure could ultimately secure temtum beyond levels seen with existing networks, without the need for expensive energy consumption.

Although the environmental impact of fuel-powered vehicles is of some concern, making use of technology that’s already in use and reducing the burden of such networks as Bitcoin on international energy resources is a positive move before more sustainable vehicles begin participating in the temtum network.

Use case - In-carwallet

The future of motoring is evolving as fast as emerging industries like Blockchain and AI. This opens up enormous opportunities when all of them are combined to improve safety, efficiency and performance.

temtum is actively exploring use of Temporal technology and temtum as an automatic payment system in the automotive industry. In its simplest form, a car having its own wallet opens up opportunities – from ANPR payments on toll roads to pay-per-mile insurance; from in-car entertainment packages to integrations with transport initiatives at both commercial and governmental levels.

Fitbit Ionic

We developed an application to load on the Fitbit Ionic smartwatch. The purpose of this application is to notify a user when they have received temtum from other users. We intend to further develop this application to allow for transactions to be sent from the smart watch.

DJI spark

Similar to the BMW i8 case, we conducted an experiment to determine whether a drone would be able to confirm transactions while in flight. Unlike the BMW it was not a full node, but it did use the CPU resources to confirm transactions sent to it from a ground station.

Due to the much lower resources of the drone, a full node was not able to run on the drone, but the drone was still able to average 270 TPS.

Homomorphic encryption and anonymity of votes

We have identified and are working with third party applications where Temporal blockchain will be used to store votes using Homomorphic encryption. Homomorphic encryption is one of the two main structures for e-voting protocols, but the encryption is only one part of the protocol.

This type of encryption is perfect for voting systems because it can perform mathematical calculations without knowing the real number of votes received. Therefore, you can add every user's votes and only the authorized user will see the result of all of them.

All results will be able to be checked by calculating it, but they won't be able to see who voted or how many votes each user sent, with the blockchain storing all votes.

What is homomorphic encryption?

Homomorphic encryption is especially good at tallying. Each voter encrypts his/her vote (a zero or a one). Since the vote is encrypted, it can be managed easily: there is no problem in associating the vote with the voter. So, the votes can be accumulated on a public bulletin board and everybody can check that his/her own vote is taken into account, or that nobody voted twice. When all the votes are obtained, homomorphism is applied to get the encryption of the sum of the votes, and the sum is then decrypted; the decryption private key is split among a few partially trusted authorities, who collaborate only for this single decryption. As long as at least one of the authorities is honest, the individual votes cannot be decrypted, and vote anonymity is maintained (we cannot know who voted what).

The challenge in such systems is how to make sure that an encrypted vote is really the encryption of a 0 or a 1, and not the encryption of something else. Practical protocols for e-voting which rely on homomorphic encryption use non-interactive zero-knowledge proofs, which are rather technical but in essence say: with sufficient mathematics thrown at the problem, it is possible, for some asymmetric encryption algorithms and with the cooperation of the voter himself, to prove that an encrypted value is really the encryption of a 0 or a 1 but not of anything else. This, of course, cannot be done without the cooperation of the voter himself, otherwise it would be a gross weakness of the encryptionsystem.

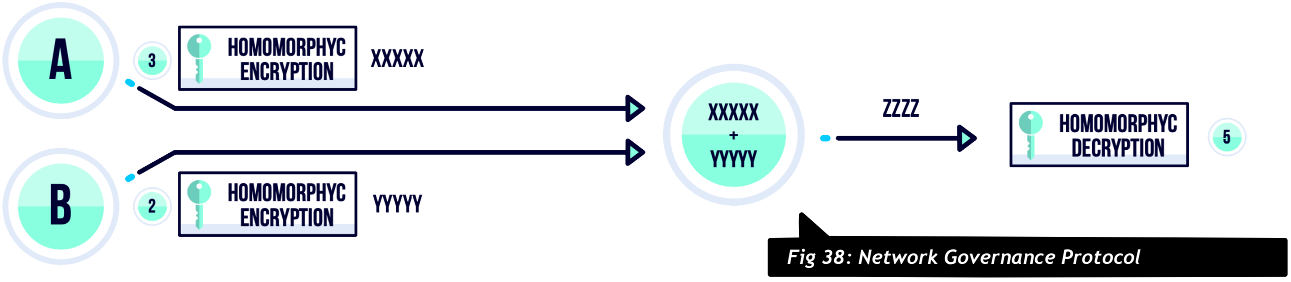


Fig 38: Network Governance Protocol

Existing payment system integration

This section outlines our detailed and systematic strategy for implementing all the financial system integration and key network technology integration required for the successful running, and mainstream adoption, of the temtum network.

Description

One of the most important factors for successfully achieving our goal of widespread global use of temtum as a mainstream form of currency is to fully and seamlessly integrate it with the methods that people already use in their daily lives: for buying and selling and for use with credit and debit cards. The components have been designed in a way that means that this currency can be used in a similar way as a fiat currency.

We have outlined above many of the top level considerations for real-world integration with conventional payment systems. This section offers a more in-depth road map of integration tasks. We are currently working with several payment services providers and expect to be able to announce a fully working system in the near future.

Benefits

Our integration model is a pioneer in the cryptocurrency world, since, unlike other cryptocurrencies, temtum is being specifically designed to coexist transparently with other fiat currency, in order to achieve the highest possible rate of adoption.

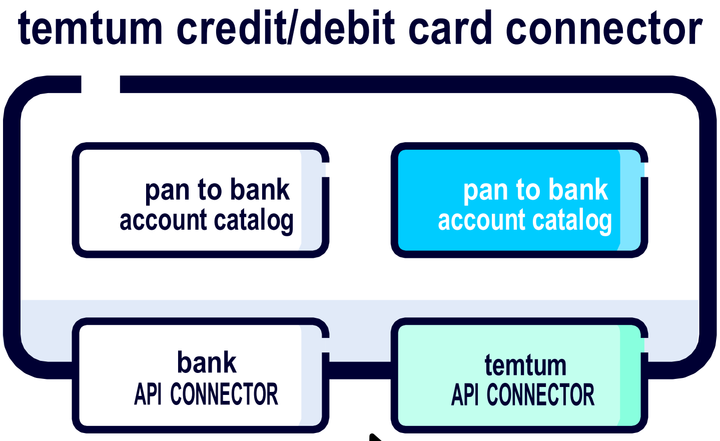

temtum credit/debit card connector
pan to bank account catalog
pan to bank account catalog
bank API CONNECTOR
temtum API CONNECTOR

Fig 39: temtum payment card connector

This software component receives transactions from the temtum network gateway, validating them and processing the fiat transaction with a special component for linking credit and debit cards' data with the wallet address.

It also contains all the credit card and debit card API Connectors, which are responsible for connecting the temtum Network to the credit and debit card system and sending the fiat transactions to the receiver credit or debit card. In the same way, this component contains all the crypto API connectors, which are responsible for connecting the temtum Network to any cryptocurrency API and sending the crypto transactions to the receiver wallet address.

Private fiat bank context

Finally, in this context, private banks will receive the transactions through internal gateways (ESB, queues, web services, files, etc.) and after transforming, formatting and internal validation, the transaction will be sent to the recipient's account.

In this context, all the systems, components and applications (web, desktop, ATM, mobile app) connected to the private bank core are involved.

temtum national bank credit and debit card system

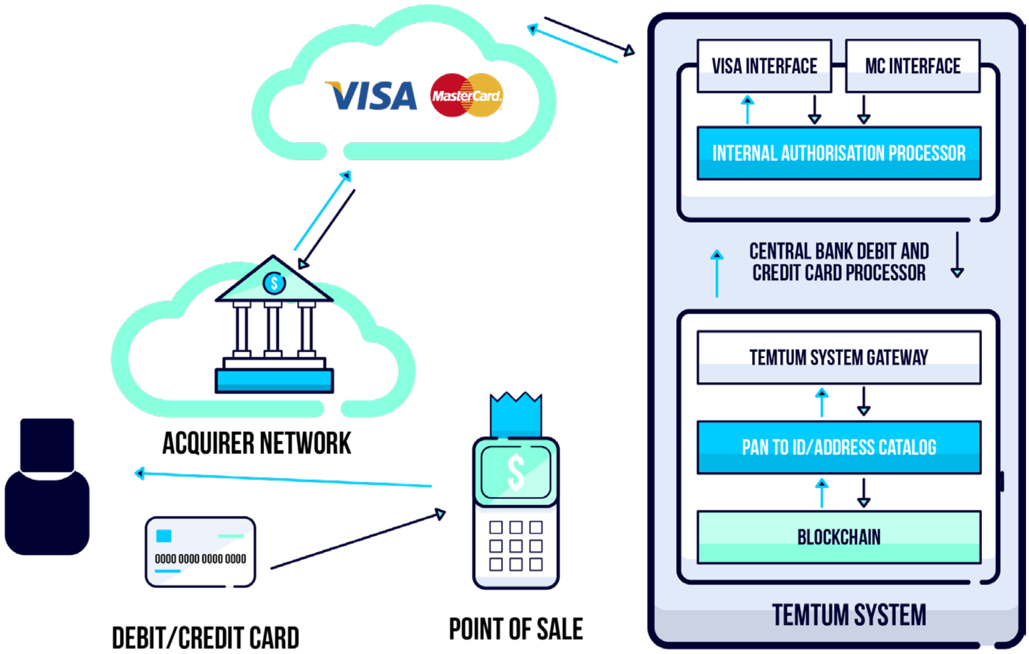


Fig 40: temtum credit/debit card system

This software component can process all the credit and debit card transactions from any part in the world. This software component can be deployed in conjunction with Visa and MasterCard franchises. Inside this module, VISA and MasterCard would install a special component that makes it possible to send and receive cryptocurrency transaction messages.

Network technology

Increased sources of randomness

Currently the Temporal Blockchain Network relies on the NIST Randomness Beacon for a quantum source of randomness. This is an excellent source of mathematically proven randomness but relying on a single source is not optimal. For example, if the NIST beacon went offline for whatever reason this would not prevent the network from functioning, but it would represent an inconvenience.

Our roadmap plans to reduce our reliance on one single source of randomness whilst maintaining all the randomness properties of the NIST Beacon. To do this we intend to incorporate the randomness beacon developed by the University of Chile whilst also developing our own in-house random source that is based on the same principles as the NIST Beacon. A nationally certified random number generator is now commercially available, and this can be incorporated into a new beacon working in collaboration with an identified academic institution. We intend for this beacon to be made publicly available, also at no charge.

This will in no way improve the randomness of the NIST random number, since the current method is proven to be random, but it will futureproof the network.

Smart contract platform

We intend to create a platform for developers to create and deploy applications onto the Temporal Blockchain. This would be coded using a standard programming language working with the community.

While limitations such as TPS limit the effectiveness of other smart contract platforms because of the unique architecture of temtum, large applications can be deployed onto the temtum network with no negative impact on the fundamental network.

We intend for TEM to be used as the currency for these smart applications and contracts.

Anything that runs on a blockchain needs to be immutable and must have the ability to run through multiple nodes without compromising its integrity. This means that smart contract functionality needs to be threethings:

- **Deterministic**
- **Terminable**
- **Isolated**

Feature #1: Deterministic

A program is deterministic if it gives the same output to a given input every single time. E.g. If 3+1 = 4 then 3+1 will ALWAYS be 4 (assuming the same base). So, when a program gives the same output to the same set of inputs in different computers, the program is called deterministic.

There are various instances when a program can act in an un-deterministic way:

- **Calling un-deterministic system functions:** When a programmer calls an un-deterministic function in their program.
- **Un-deterministic data resources:** If a program acquires data during runtime and that data source is un-deterministic then the program becomes un-deterministic. For instance, suppose a program that acquires the top 10 Google searches of a particular query. The list will be likely to change over time.

- **Dynamic calls:** When a program calls the second program it is called dynamic calling. Since the call target is determined only during execution, it is un-deterministic in nature.

Feature #2: Terminable

In mathematical logic, there is an error called the 'halting problem'. It states that there is an inability to know whether or not a given program can execute its function within a time limit. In 1936, Alan Turing deduced, using Cantor's Diagonal Problem, that there is no way to know whether a given program can finish in a time limit or not.

This is obviously a problem with smart contracts because contracts, by definition, must be capable of terminating in a given time limit. There are some measures taken to ensure that there is a way to externally 'kill' the contract so it does not enter into an endless loop, which will drain resources:

- **Turing incompleteness:** A Turing incomplete blockchain will have limited functionality and will not be capable of making jumps and/or loops. This means they cannot enter an endless loop.

- **Step and fee meter:** A program can simply keep track of the number of 'steps' taken, i.e. the number of instructions it has executed, and then terminate once a particular step count has been executed. Another method is the fee meter. Here the contracts are executed with a prepaid fee in which every instruction execution requires a particular amount of fee. If the fee spent exceeds the pre-paid fee, then the contract is terminated.

- **Timer:** Here a predetermined timer is kept. If the contract execution exceeds the time-limit then it is externally aborted.

Feature #3: Isolated

We are developing a compiler and interpreter to allow the code for smart contracts to be run in a sandbox environment on the blockchain. Thus, any unexpected issues with the smart contract code, which can be uploaded by any third-party, will not affect overall network performance.

The intended goals of the temtum smart contract platform are:

- **Support for millions of users:** The system must be able to scale to millions of users. This is especially true for DApps (decentralised applications) that are looking for mainstream acceptance

- **Free of charge usage:** The platform should enable the developers to create DApps which are free to use for their users. No user should have to pay the platform to gain the benefits of a DApp.

- **Easily upgradable:** The platform should allow the developers the freedom to upgrade the Dapp as and when it is desired. Also, if any Dapp is affected by a bug, the developer should be able to fix the DApp without affecting the platform.

- **Low latency:** A DApp should run as smoothly as possible and with the lowest possible latency.

- **Parallel performance:** A platform should allow their DApps to be processed in parallel in order to distribute the workload and save up time.

- **Sequential performance:** Not all the functions on a blockchain should be done in parallel. In the context of actual transaction execution, multiple transactions cannot be executed in parallel; they should be done sequentially to avoid errors such as double-spend.

Leader Selection Algorithm

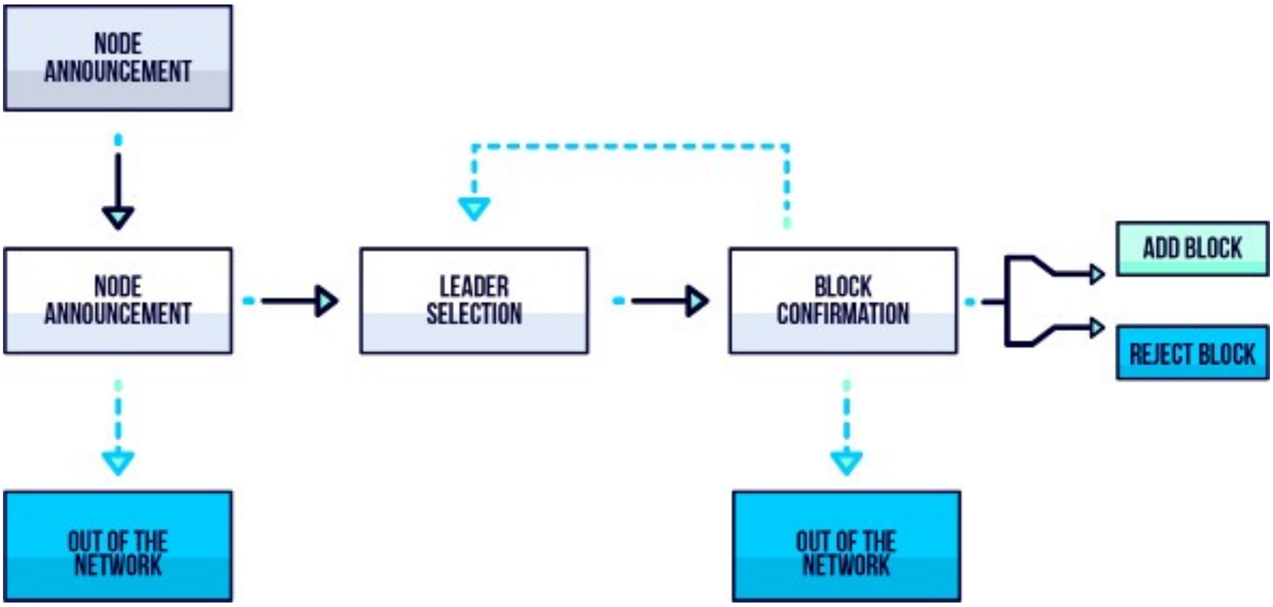


Fig 41: Leader Selection Algorithm

The Leader Selection Algorithm uses a three-phase process to avoid a Sybil attack at low cost:

» Performance Integrity Protocol: This protocol is designed to ensure that the leader node has adequate resources to meet the demands on the network. It is also undesirable to have low-resourced nodes confirming blocks because they may be slow and permitting low resourced nodes to be the leader reduces the costs for a potential attacker. Therefore, the network will test nodes to verify if they have enough resources to act as leader. Other lower resourced nodes which are not qualified to become the leader node will continue to support network integrity and security by maintaining a local copy of the Temporal Blockchain.

» Leader selection: A random quorum of nodes will be selected to confirm/reject blocks for the interval.

» Block confirmation: Submitted blocks will be validated before being added to the blockchain.

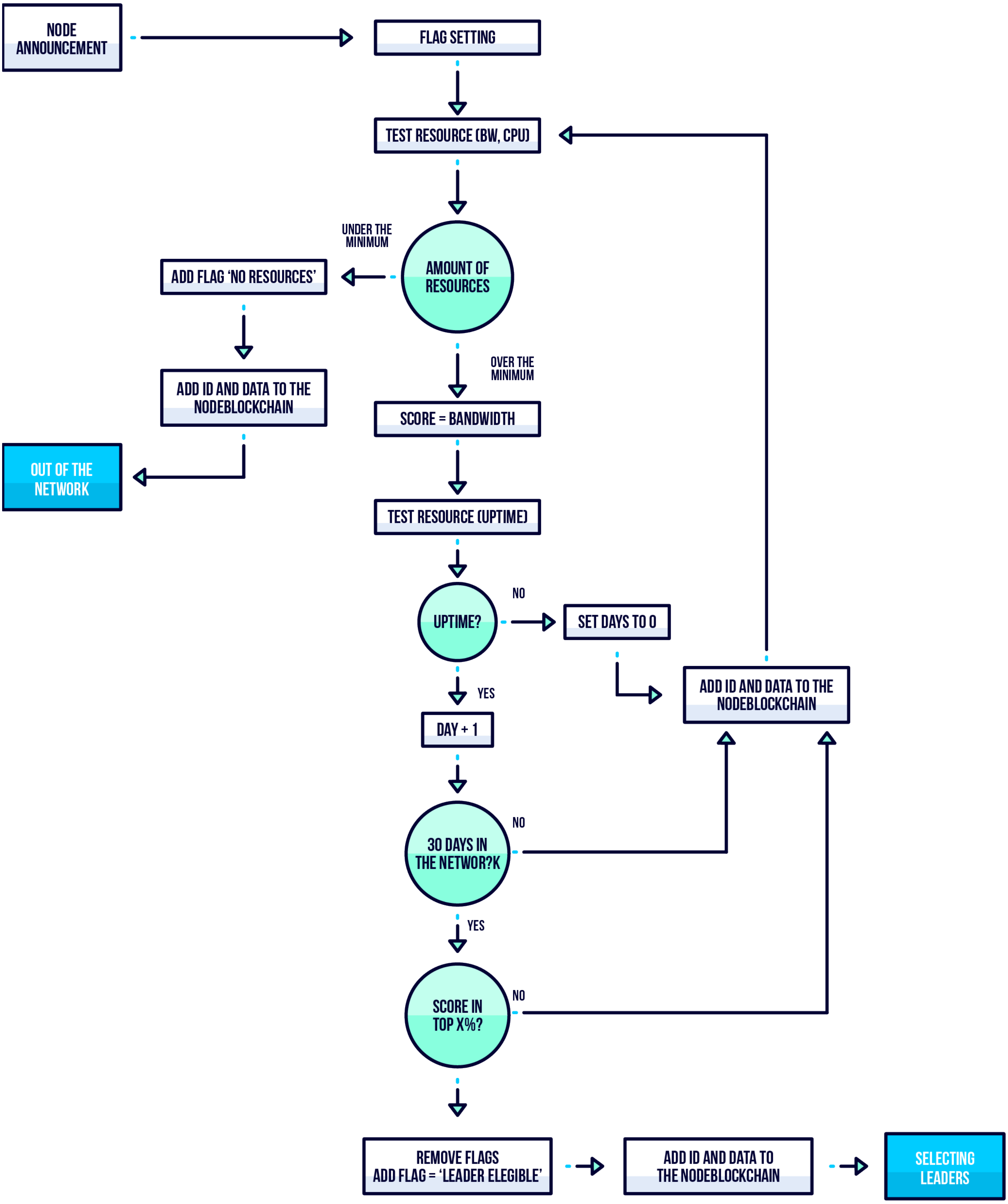


Fig 42: Performance Integrity Protocol / Node selection 1

Phase 1: Performance Integrity Protocol

To join the network, a node must reach a threshold in a resource test. The network will test the node and then grant it certain flags to identify if it is a new node or leader-eligible.

Therefore, the leader nodes that will agree on and sign the NPD will be the most trusted nodes on the temtum network and have the longest tenure. Authority nodes therefore have no economic incentive to operate maliciously, as they do not participate in any mining or transaction confirmation.

The following describes in detail the steps in the phase 1 diagram below:

Node announcement: Every new node must announce itself to an authority node.

- Each node must send its public key, software version, machine configuration/capabilities and IP address to the authority node.
- Certain data will also be supplied:
- **Operating system** (for informationonly)
- **Uptime:** Amount of time a node has stayed up and running, so it can be relied upon.

Flag setting: The authority node will set the following flags:

- **'Untested':** This will help the network to identify that the node has not passed the number of tests necessary to be considered a new node.
- **'New Node':** This will help the network to identify that the node has not been in the network for at least 30 days.

Resource evaluation (BW, CPU): Before joining the network, every new node must be tested to verify that its resources are sufficient (test).

Test frequency: Each test will be conducted once every 24 hours by an authority node or another node delegated for that task but trusted by the authority nodes. It may be undesirable to do these tests on a bandwidth node because it may constrain their resources. Tests should be run at an unpredictable time each day. In the case of:

- **BW/CPU failure, the node will be removed from the network.**
- **Uptime failure, the node will be set as 0 days in the network.**

CPU resource test: So that the authority nodes can test the available CPU capacity, they will generate a random 64-bit nonce. They will then send this to the node intended to be tested who will hash it (by concatenation) with another zeroed nonce of equal length. This additional nonce will be incremented until the result from the hash has the first X number of bits set to zero.

result = SHA512(DirectoryNonce || AdditionalNonce)

(|| means concatenation)

Both nonces will be returned to the authority node, which will verify the correctness along with a record of the time taken to calculate the result, and store this with the node information as the 'MEASURED CPU.'

If the node returns an invalid result, then the node will be excluded from the network after three re-attempts producing the sameresult.

Bandwidth resource test: To test a node's bandwidth, an authority node will send the node a large quantity of data which the node will calculate the rolling hash for (using SHA512). As soon as the node has received the final piece of data then it will send the resulting hash back to the authority node who will verify its authenticity. The quantity of data in kilobytes will be divided by the time taken to send the data and recorded as the node's 'MEASURED BANDWIDTH.' If the authority node finds the hash invalid, the node will be excluded from the network after three re-attempts producing the same result.

Uptime measurement: When a node first joins the network, the date and time is recorded with the node's entry which enables uptime calculation. If a node fails or does not respond to a bandwidth test, this date and time is reset to the current time. After four failed attempts (as specified above) the node is deleted from the network.

Score = Bandwidth: The bandwidth measurement in kilobytes per second will be set as the score, which will then be used to grant flags.

Add ‘no resources’ flag: If the node does not have enough resources:

- **All flags are removed.**
- **A new flag is added as ‘no resources.**
- **The node will be removed from the network.**

Add ‘leader-eligible’ flag: If the node has passed 30 days in the network and the score is in the xxth percentile.

- **Flags are removed: ‘Untested’, ‘NewNode’.**
- **Flags are added: ‘leader-eligible’.**
- **Adding the node to data-blockchain:**
- **In order to keep records on every node’s data, the public key, IP, OS, flags and other information (days in the network and score) will be added into the data-blockchain. This data can be used as an input to develop the machine learning and for verification by any node.**

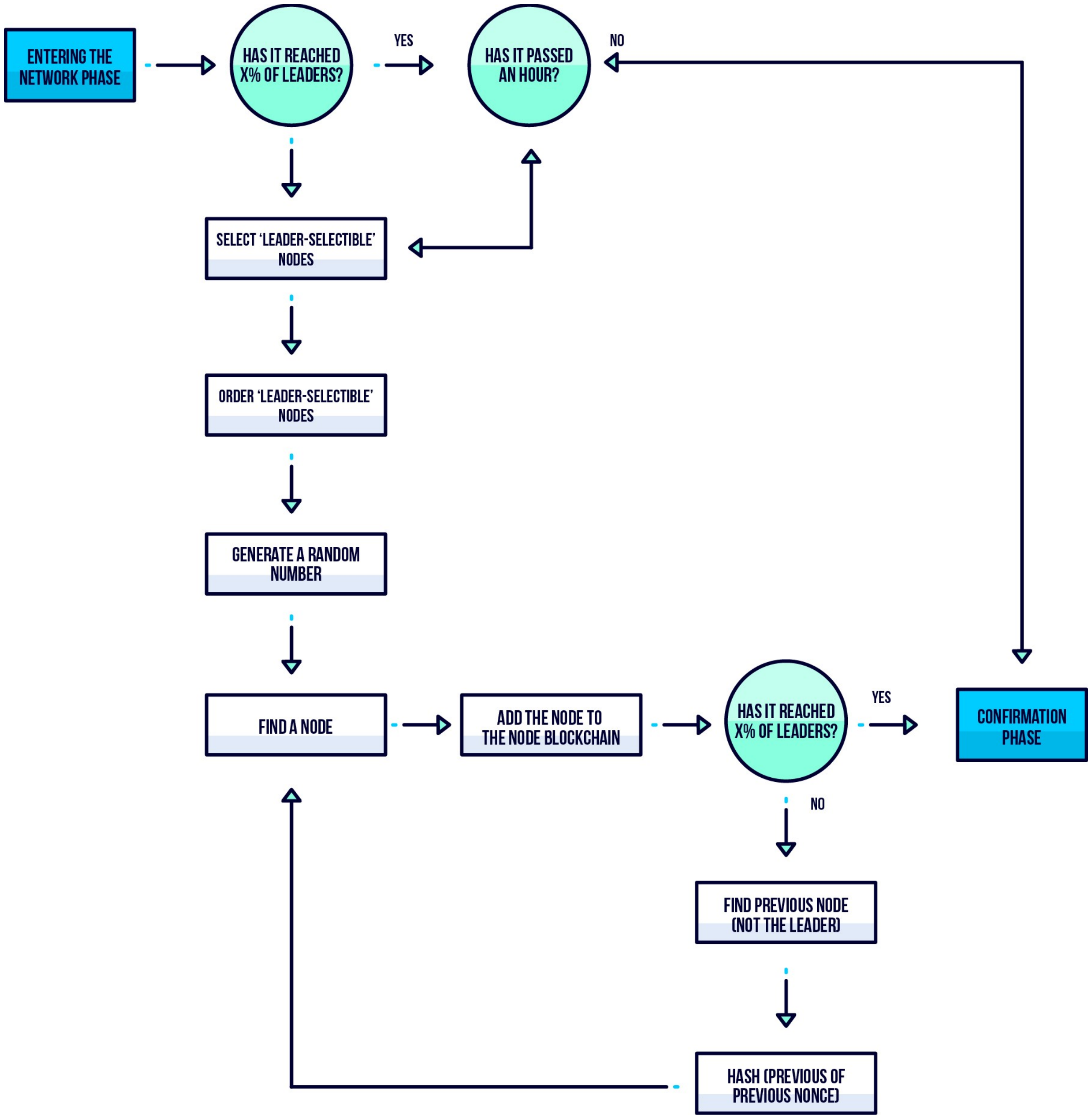

ENTERING THE NETWORK PHASE
HAS IT REACHED X% OF LEADERS?
YES
HAS IT PASSED AN HOUR?
NO
SELECT 'LEADER-SELECTIBLE' NODES
ORDER 'LEADER-SELECTIBLE' NODES
GENERATE A RANDOM NUMBER
FIND A NODE
ADD THE NODE TO THE NODE BLOCKCHAIN
HAS IT REACHED X% OF LEADERS?
YES
CONFIRMATION PHASE
NO
FIND PREVIOUS NODE (NOT THE LEADER)
HASH (PREVIOUS OF PREVIOUS NONCE)

Fig 43: Node Evaluation 2

Phase 2: Leader Selection

Using all nodes with the 'leader-eligible' flag, the network will randomly select x% nodes of the network to be leaders and confirm blocks. The resulting number of nodes must be odd, and so if the percentage yields an even number of nodes, the network simply increases the requirement by one node. This phase will be updated every hour.

Selecting 'leader-eligible' nodes: We will have to look for nodes with the 'leader-eligible' flag because they have been tested and scored as the top nodes with the best resources, which can be selected as leaders.

Order 'leader-eligible' Nodes: Before selecting them as leaders, it is important to order them (ascending or descending) according to their public key hash.

Generate a random number: This random number will help us select the first node.

Find a node: The network orders all leader-eligible nodes in the network by their public key and then choose the node with the next largest integer value above that hash of the random number (also used as an integer).

Adding the node to data-blockchain: In order to keep records on every node's data, the public key, IP, O.S, flags, uptime and score will be added into the Data-Blockchain. This data can be used as an input to develop the machine learning.

Find the next node: If we have not reach x% of leaders needed to confirm a block, it will need to find the next node of the set. To do this, we take the previous hash and hash it again, and repeat the find node step above. We hash the previous hash rather than the public key of the chosen node because hashing the public key of the node will generate an undesirable repeating cycle.

Hash (previous hash): To find a new leader node we will have to hash the key of the previous node.

Note: *The line between the confirmation phase and the selection leader phase happens only when something irregular happens (see 'block confirmation').*

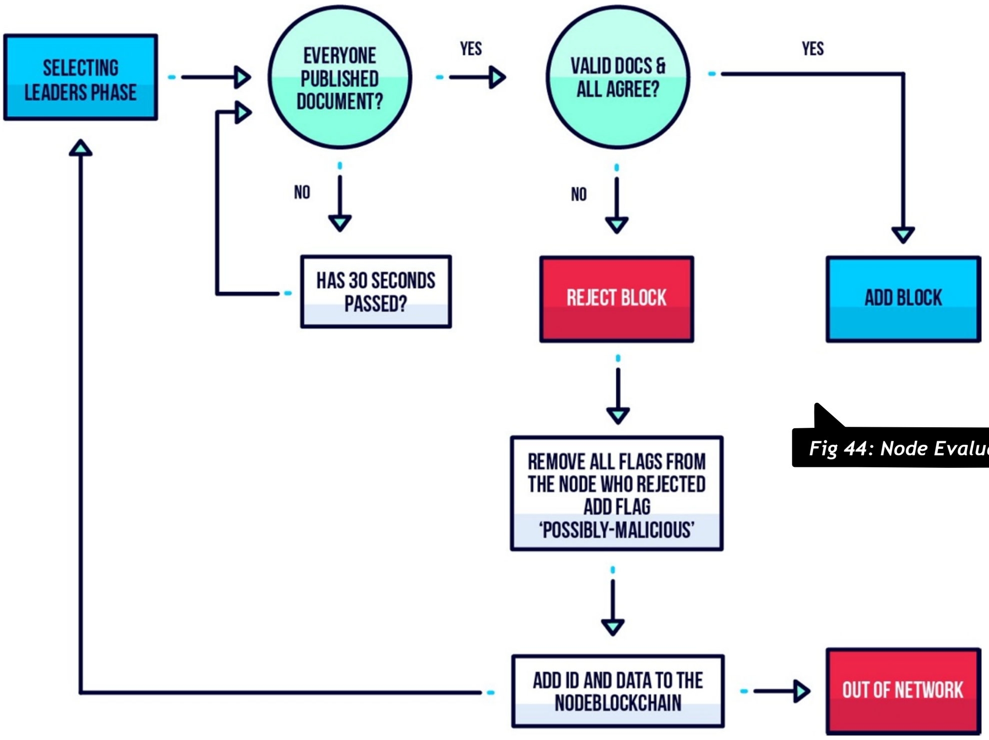

SELECTING LEADERS PHASE
EVERYONE PUBLISHED DOCUMENT?
YES
VALID DOCS & ALL AGREE?
YES
NO
NO
HAS 30 SECONDS PASSED?
REJECT BLOCK
ADD BLOCK
REMOVE ALL FLAGS FROM THE NODE WHO REJECTED ADD FLAG 'POSSIBLY-MALICIOUS'
ADD ID AND DATA TO THE NODEBLOCKCHAIN
OUT OF NETWORK

Fig 44: Node Evaluation 3

Phase 3: Block confirmation

After selecting the leaders, the network asks them to confirm the block in order to add it or not to the blockchain.

It is important to:

- **First, wait for every leader node at least 30 seconds to publish their document.**
- **Second, verify if all published documents are in agreement. A disagreement will tell the network if a node is possible-malicious or not; if so, it will be taken out of the network.**

- **If a disagreement occurs, the decision (add/reject block) will be made based on the what the majority of the nodes decided.**
- **Finally, if all documents are valid, depending on their full agreement, we will have to add the block or reject it.**

Double blockchain

With the current system the network issues an NPD document, which is signed and distributed to all nodes. In the future we intend to create a double blockchain system using a secondary blockchain and exploiting the Temporal algorithm to reduce the size of the chain.

This blockchain will only be appended to by the directory authority and will contain data from the candidate eligibility system described above.

The reasons for using a blockchain system to store this data include:

- **enabling more efficient distribution of the data;**
- **a perfect audit trail that is attack resistant; and**
- **to provide inputs to the intrusion detection algorithm to defend against Sybil attacks.**

Intrusion Detection Algorithm

The purpose of our Intrusion Detection Algorithm is to provide an extra layer of security to allow the temtum network to determine patterns of behavior of all the nodes in the network, detecting malicious nodes and preventing attacks.

The patterns will be determined by using the information obtained from each node added to the network or selected as a leader. This data will be recorded on a secondary blockchain to help us build, train and test the Intrusion Detection Algorithm, providing temtum with unique AI protection in real time.

The algorithm needs to be built and trained by a percentage of network data and tested with a different subset of it. Most existing networks use different methods to challenge and detect malicious nodes in their networks.

We intend to create a model that will predict and prevent malicious nodes from ever being a part of the temtum network. Data from trusted nodes can be very useful to establish the behavior of honest-nodes by creating a prediction model. The data used can vary, from the userID or IP address (where it comes from) to the time connected and decision making. Any type of data from a node can add value to the model and increase its accuracy of detection over time and through network scaling.

Sharding and delegation

We have conceived a unique method to allow a main node to temporarily delegate its authority to other nodes in order to increase the number of transactions that the network can process.

- **Step 1 – decide which node(s) the leader can delegate to**
- **Step 2 – determine how to delegate the authority securely. This addresses the need for a delegated node to appear like a leader node to the network.**
- **Step 3 – reassemble the data into a cryptographically valid block by a unique method.**

This would allow for an increased number of TPS to be achieved because the network can use otherwise unused resources.

Process for ISO 27001 accreditation (information security)

temtum intends to register for ISO 27001:2013 in due course. The ISO (International Organization for Standardization)/IEC (International Electrotechnical Commission) 27001:2013 is recognized as an international foundation standard that provide the requirements for implementing, maintaining and continuously improving an Information Security Management System (ISMS).

The ISO 27001:2013 standard has been adopted by many companies as a strategy to protect information from misuse, unauthorized disclosure, damage or loss. Therefore, temtum is in the process of adopting an ISMS as an additional security layer to preserve the confidentiality, integrity and availability of information. Policies and procedures are being implemented and documented to protect information from vulnerabilities, threats and risks, whether internal or external, deliberate or accidental.

The confidentiality, integrity and availability (CIA triad) of information in the ISMS are integral parts of its management function and views these as their primary responsibility and fundamental to best business practice.

Therefore, it is important for temtum to implement this to ensure:

» **Information is protected against unauthorized access and unauthorized modification.**

» **Information is not disclosed to unauthorized persons through deliberate or careless action maintaining confidentiality.**

» **Availability of information to authorized users as and when needed.**

» **Regulatory and legislative requirements will be met.**

» **Business continuity plans are produced, maintained and tested as far as practicable.**

Some of the policy statements that are been documented to ensure the CIA triad of information:

» **Password controls: Includes guidelines (frequency of change, length, complexity) of passwords used on temtum's systems and/or services.**

» **Resource usage policy: Establishes guidelines, according to the type of user, to use any of temtum's resources.**

» **Data privacy: Sets out rules for managing personal data to be followed by the directors and employees of the company, and to ensure the confidentiality and integrity of sensitive data.**

» **Web application security: Establishes controls to analyze and test vulnerabilities from the user perspective.**

» **Vulnerabilities control policy: Establishes a guideline in order to analyze the infrastructure in terms of vulnerabilities, and to priorities remedial actions to manage the identified risk.**

» **Security breach and incident management: Explains how to respond to any security breach or incident. All threats found must be analyzed, documented and managed following this guideline.**

» **Human resources security: Defines the rules to be followed before, during and after the termination of employment of all employees, consultants and contractors, third parties and/or associates.**

» **Third-party risk management: Guidelines that third-parties must comply with in order to work with temtum.**

Conclusion

temtum

Cryptocurrency. Evolved.

We believe that temtum represents a remarkable new opportunity beyond even a step-change for blockchain and the first mass-adoption of a cryptocurrency. In fact, we believe that temtum can form the basis of an entirely new – and better – way of structuring financial relationships that is more environmentally friendly, transparent, traceable, secure and reliable than existing cryptocurrencies.

We have outlined in this paper how the fundamental values and principles of blockchain have been compromised in the cryptocurrency space due to inherent flaws in the existing technology. This has meant that blockchain cryptocurrencies have not delivered the user benefits they promised and, largely as a direct consequence of this, have failed to achieve widespread adoption.

temtum's technology builds on previous blockchain theory but represents a significant evolutionary leap from previous technology, which delivers an enhanced experience in terms of speed, resource-use, energy costs, environmental impact and true decentralization. Our work in quantum randomness also ensures completesecurity.

Exploring opportunities within existing markets such as gaming and e-commerce, has opened new opportunities for temtum to provide payment solutions to high transaction platforms, who will directly benefit from the innovations that underpin its proprietary technology.

As we have demonstrated above, this groundbreaking cryptocurrency has been fully developed, deployed and tested and is ready for full integration with existing payment systems to ensure the seamless adoption of temtum by regular consumers.

Our vision is a positive one. We believe that temtum will not only transform the blockchain and cryptocurrency markets; it will make the world a better place for more people. That is our purpose and we have a truly world-class and dedicated team that is fully committed to achieving it. We invite you to join us on our exciting journey to the future of finance.

The Team

temtum

Cryptocurrency. Evolved.

Core Team

Richard Dennis - *Chief Executive Officer*
Richard is the founder of Dragon, and a globally acknowledged, prolific and prodigious cybersecurity and cryptography expert. He is also internationally recognized as one of the world's leading cybersecurity lecturers with a specialism in secure networks, blockchain and encryption. He has a significant body of published research, cited 100's of times within Blockchain, and presentations on next-generation solutions across a wide range of subjects, including Bitcoin wallet vulnerability, an analysis into the scalability of Bitcoin and Ethereum, and a formal analysis of the Temporal block.

Dr Gareth Owenson- *Chief Information Security Officer*
Gareth holds a PhD in Computer Science and a BSc in Internet Technology and is a specialist in internet security, cryptography and distributed systems. He has conducted research in large distributed systems with a particular interest in cryptographic applications such as darknets and digital forensics, including developing automated analysis techniques to rapidly reverse engineer advanced malware to determine its functionality and develop countermeasures. He has authored many publications in journals and conferences and regularly serves as a referee for Elsevier, IEEE and CHINACOM. He has conducted a large study into the use of darknets; he is widely recognized as an expert in this field and frequently speaks on this topic. He has also advised the UK and US governments on darknets and internet filtering policy.

David Hodkinson - *Chief Financial Officer*
David is the co-founder and CEO of Harvex, a specialist firm working with clients in the cryptocurrency, blockchain and online gaming sector. He has worked with multiple high-value ICO's, advising on international structuring, banking and tax. As a qualified accountant, he has overseen the financial affairs of a wide range of cryptocurrency companies. Alongside this, he has been involved in the strategic launch of multiple online gaming companies and the integration of cryptocurrency with these platforms.

Cyntia Aguirre - *Chief Software Architect*
Cyntia is a Master of Science in Software Engineering with a strong background in software development and IT architecture. She has four years' experience both developing as a full stack developer and designing and implementing software as an IT architect for the financial industry (Banco del Austro S.A.). She also holds a PMP accreditation (Project Manager Professional) certified by the Project Management Institute USA.

David Shimmon - *Director*
David Shimmon is a highly experienced CEO of the highest caliber. His last role was as CEO of Ichor Systems, Inc, one of the world's leading semiconductor businesses. He was also CEO of global digital technology agency Celerity from 1999 to 2008, executive chairman from 2000 to 2008 and executive director from 2000 to 2008. Prior to this he had a number of other senior roles, including president of Kinetics Group, Inc., a subsidiary of Celerity, Inc. from 1996 to 2005, CFO from 1991 to May 2005, and COO from 1990-1991. He has also been the director of The Tech Museum of Innovation in California.

Campbell Law - *Director*
Campbell is the managing director of Beacon Management (Cayman) Ltd and has over 25 years' experience in the financial services industry. He has considerable experience working with both offshore and local businesses and has specific expertise with local company set up and licensing, fund administration, corporate governance and regulatory risk management. Campbell has sat on various Cayman Islands Government Boards including the Trade and Business Licensing Board and is the former chairman of the Liquor Licensing Board along with review committees for both the Trade and Business Licensing Law and the Local Companies Control License Law. Mr. Law is a Notary Public in the Cayman Islands.

Kanika Green - *Director*
Kanika is the managing director/CEO at Corporate Management Solutions (Cayman) Ltd, a fiduciary boutique. Mrs. Green is an approved director and Anti-Money Laundering Reporting Officer by the Cayman Islands Monetary Authority (CIMA). Mrs. Green has a law degree (LLB Hons.) from University of Wolverhampton in the UK which she completed in 2007, and was called to the bar in 2014. Mrs. Green's professional memberships include: Member of the Caymanian Bar Association, Member of the International Bar Association, Member of the 100 Women in Hedge Funds, Notary Public for the Cayman.

Developers

Eugene Zimnitskiy - *Lead Developer*
Senior/Team Lead Full Stack Developer. Stack of technologies: JavaScript, TypeScript, NodeJS, Angular, VueJS, React Native, React, HTML, CSS, Apache Cordova, AWS, MongoDB, LMDB, Blockchain, MySQL, MSSQL, PostgreSQL, PHP, C#, Ruby. He has been developing applications for over 8 years and projects include cross-platform mobile applications, chatbots, desktop, finance and more.

Egor Veremeychik
Egor is an iOS developer. He has over four years' experience in software development. His core technology is iOS. Egor is responsible for writing temtum applications, and for developing and supporting the iOS application. His main tasks include the implementation of data, views, logic layers, bug-fixing, performance and security optimisations.

Languages: Swift. Technologies and tools used in iOS application: CoreData, Alamofire, DeepLinks, WebSocket, XCTest, Cocoa Pods, Keychain, Firebase Messaging, Fabric, Crashlytics.

Alex Yalovik
Alex is principally an Android developer, with three and a half years' experience in software development. His core skill is Android. He is responsible for writing the temtum platform, and he develops and supports the Android application. His tasks include the implementation of new features, UI layout, bug-fixing, performance and security optimisations.

Technologies and tools used in Android application: RxJava, Mvp, SafetyNet, FCM, DBFlow, SQLiteCipher, Android KeyStore, Retrofit, OkHttp, Bamboo, Figma, Fabric, WebSocket, Robolectric, JUnit.

Andrey Vladyko
Andrey is an Android developer with eight years' experience. His stack of technologies includes: RxJava, Mvp, SafetyNet, FCM, DBFlow, SQLiteCipher, Android KeyStore, Retrofit, OkHttp, Bamboo, Figma, Fabric, WebSocket, Robolectric, JUnit. His tasks included designing the application architecture, UI Layout, bug fixing, performance and security optimisations.

Artem Koush
Artem is a web developer. His stack of technologies includes: JavaScript, TypeScript, NodeJS, Angular, VueJS, HTML, CSS, jQuery, Apache Cordova, Ionic Framework, MongoDB, MySQL, PostgreSQL. He has been developing web applications for four years. His projects included cross-platform mobile applications, chatbots and more.

Illia Zabrodski
Illia is a full-stack JS developer with extensive experience, management and teamwork skills. As a developer with around five years creating awesome software, he has mastered web development and uses a highly scientific approach to coding. He applies the latest technologies and know-how to make the project work.

His stack of technologies includes: JavaScript, TypeScript, NodeJS, Angular, VueJS, HTML, CSS, React JSMongoDB, MySQL

Bo Lasater - *Senior Product Advisor*
Bo's 20+ year career in Silicon Valley has focused on product design and engineering. He started as an engineering manager at Morgan Interactive, one of the early leaders in multimedia entertainment, and eventually became a designer and producer. In the late 90s and early 2000s, he co-founded two successful sister companies, Fort Point Partners and Totality. Fort Point built high-performance e-commerce sites and Totality provided systems integration and application management services for them. Totality raised over $100m and was eventually sold to Verizon. Since then, Bo founded SuperEgo Games, a company that developed console episodic content for Sony's PlayStation network. He also ran the Reputation project at MySpace. Currently, Bo heads engineering and product at Mido Play, a venture he co-founded that is building a social-mobile platform for lottery applications.

Johannes Fröhling– *Technology Advisor*
After spending his whole career working in the strategy departments of public high-tech companies – mainly in the semiconductor and display sectors – he founded his own investment company running merger and acquisition projects with a strong focus on deeptech. He works with leading venture capital companies, private equity firms and private investors on a global basis. Johannes can rely on his global experience and network which he has generated working for over three years in China at Grace Semiconductor and a further three years in the USA at Applied Materials. Beyond that he lived and worked in India and Japan for several years. Johannes holds an MBA and a Graduate Engineering degree in semiconductor technology.

Rupert Boswall, RPC - *Legal Advisor*
Rupert is RPC's senior partner, a non-executive chairman role. Rupert acts on high-value international disputes and investigations in the financial, technology, infrastructure, natural resources, offshore and wealth sectors. He is noted for his lateral thinking and strategic leadership of teams on cross-border projects. Although a litigator by background, he is a solver of clients' issues in deal making as well as disputes. Rupert has particular experience acting for clients from Africa, Russia, the CIS, the Middle East, the PRC and SE Asia. He is dual-qualified in England and Wales, and Hong Kong.

Patrick Ormond*, Legal Advisor*
Patrick advises financial institutions, corporates, funds and investors on international finance and corporate transactions. His finance experience includes advising both lenders and borrowers on a wide range of bilateral and syndicated transactions, including real estate finance, construction finance, project finance, structured finance, acquisition finance and general corporate financings. His corporate experience includes advising on mergers and acquisitions (including take-privates), joint ventures, IPOs and corporate reorganizations.

Nicola McKilligan-Regan – *Data Privacy and GDPR Advisor*
Senior Partner at Privacy Partnership and CEO Founder of SmartPrivacy. Advisor on all aspects of data privacy law including the GDPR, cybernetics and data ethics. She is a human rights and data privacy law specialist with over 20 years' experience with multinationals and with the Information Commissioner's Office.

English law legal advice

RPC (www.rpc.co.uk) is a major city law firm with headquarters in London and offices in Bristol, Singapore and Hong Kong. RPC has significant expertise in technology, IP, investment structures, private equity, finance and tax, litigation, insurance and real estate and is ranked highly relative to peers in independent legal directories such as Chambers UK and The Legal 500.

RPC have acted for coin issuers, crypto-exchanges, blockchain developers and blockchain start-ups, and their experience includes advising on the intellectual property aspects of blockchain, IP licensing arrangements, advising on ICO fundraising and structuring, platform terms and conditions, the settlement of claims arising from hacks of major cryptocurrency exchanges, advising on the theft of bitcoin sale proceeds, including coin provenance / tracing issues, and advising cryptocurrency-related businesses and token issuers on regulatory, licensing and commercial issues.

Identity Verification / KYC Provider

ShuftiPro provides next-generation end-to-end identity verification services. It is a SaaS product offering KYC and AML verification as its basic features of operation. The hybrid artificial and human intelligence technology of ShuftiPro has the ability to verify 7 billion people living on planet Earth with 99.6% precision. ShuftiPro has engaged customers from various countries and belonging to diverse categories. Its digital KYC services have enabled its clients to identify their customers with frictionless accuracy, helping them to reduce cost overheads. ShuftiPro helps its banking and finance customers by providing AML Compliance services through a gigantic data bank that is updated every 14 minutes.

British Virgin Islands law legal advice

Walkers (www.walkersglobal.com) is a leading international law firm that provides legal, corporate and fiduciary services to global corporations, financial institutions, capital markets participants and investment fund managers. Walkers is consistently ranked in the top tier of the leading global legal directories. Walkers has created an offshore market leading FinTech team and works closely with policymakers, regulators and governments to facilitate appropriate legislation and regulation that keeps pace with innovation. Walkers has particular expertise in advising businesses specializing in blockchain, digital assets, alternative model finance and a wide range of related activities and services including funds, issuers, custodians and broker dealers.

Harvex – Crypto accounting and structuring

Harvex are a specialist international Accounting, tax and Advisory firm operating in the rapid growth sectors of Cryptocurrency, Blockchain and Online Gaming. From their offices in UK and Malta, Harvex have been at the forefront of Cryptocurrency / ICO development providing services such as international setup and structuring, banking, accounting and tax.

As highly experienced cryptocurrency accountants and advisors, Harvex have extensive and in-depth connections and knowledge in all the major worldwide crypto hotspots. Harvex have supported both corporate and individual clients, adapting to ever evolving legislation and requirements.

Within the cryptocurrency sector, Harvex's clients include crypto-exchanges, trading and investment firms, asset management funds and brokerages. Additionally, Harvex have worked on multiple ICOs, that have launched in a number of jurisdictions. Harvex's clients extend across the online gaming world, from multiple casinos and poker sites to crypto payment processors.

bsi.

Pen testing and third-party security

BSI Cybersecurity and Information Resilience (UK) Ltd is an NCSC approved company that provides penetration testing of IT systems to identify potential vulnerabilities and recommend effective security countermeasures.

A service provider can analyze the systems or networks that companies rely on to carry out their business securely and effectively by conducting a number of tests designed to identify any weaknesses using publicly known vulnerabilities and common configuration faults.

BSI’s clients include government and critical national infrastructure (CNI) customers, demonstrating that they have the highest possible standards.

BSI is also a Certified Cyber-Security Consultancy (CCSC) and we can confirm that they met our high standards for security architecture, risk assessment and risk management services.

The Certified Cyber-Security Consultancy (CCSC) scheme was developed to enable easy identification of companies capable of offering high quality, tailored, expert cybersecurity advice. Originally developed by CESG, the scheme is now operated by the National Cyber Security Centre (NCSC), which is part of GCHQ (Government Communications Headquarters).

Terms and Conditions

temtum

Cryptocurrency. Evolved.

This document (the **'White Paper'** or **'white paper'**) is issued by Great Harbour Trading Limited trading as temtum (**'temtum'**). temtum is a company registered in the British Virgin Islands under company registration number 1990517 whose registered office is at 1/F Columbus Centre, PO Box 2283, Road Town, Tortola VG 1110, British Virgin Islands. The parent company of temtum is Dragon Infosec Limited (**'Dragon Infosec'** or **'Dragon'**).

The White Paper is furnished to you on a confidential basis and should not be distributed, published or reproduced, in whole or in any part, nor should any of its contents be communicated or disclosed by you to any other person.

The White Paper is for information purposes only and is not intended to and should not be construed as an offer, commitment or undertaking, and does not constitute an offer to sell or the solicitation of an offer to buy in any state or jurisdiction.

Whilst reasonable efforts have been taken by temtum to seek to ensure that the contents of the White Paper are accurate and not misleading (at the date of writing), there can be no guarantee that the information set out in the White Paper will not be outdated or modified in the future.

All statements of opinion or belief and all forward-looking statements (including statements of intent, opinions, projections, forecasts and estimates) relating to future events or performance contained in the White Paper reflect temtum's current intent, assessment and expectation and speak only as of the date specified in respect of such statements or otherwise the date of the White Paper. These statements should not be read as commitments or as accurate indicators of future events or performance. No representation or assurance is given that any such intentions will not change, that any such statements are correct, or that any such events or performance will occur.

This White Paper is dated February 2019 and information in this White Paper relates only to periods on or prior to the date of this White Paper.

Glossary of Terms

temtum

Cryptocurrency. Evolved.

Archive node - Performs as a Temporal node whilst storing all blockchain data to be queried by other network nodes.

Authority node - Semi-trusted nodes that perform 'key certificate' document signing and create the Node Participation Document (NPD), whilst collectively ensuring integrity of each NPD.

Blockchain- A decentralised system that records transactions across a distributed ledger that is linked in a peer-to-peer network.

Block explorer – See 'Explorer'

Coin - Payment coin (or exchange coin) – a means of digital payment or value transfer

Consensus - This is a process where the majority of network participants agree on the validity of a transaction or action to maintain the integrity of a distributed ledger

Deterministic - Software is considered deterministic when it gives the same output to a given input every single time, even across multiple devices. A core feature of a smart contract.

Explorer - A visual representation of the transactions on the blockchain. Used to confirm transactions and block IDs.

Fiat (money) - Government issued money that has no intrinsic value; its value is only maintained by governments and other institutions.

Flags - Used as markers on nodes, flags help support the temtum network with data on which nodes to trust. Example flags include Untested and NewNode.

Fork - A blockchain fork is a collectively agreed upon software update, though not all forms are unanimously agreed upon by the community of full nodes.

Hard fork - A fork that is incompatible with older versions of software

Soft fork - A fork which works with older versions

Genesis block – The first block of a blockchain.

Hash/hashing - A unique identification code, generated as a transaction is committed to a block. Used to find transactions on the blockchain, usually via an Explorer.

Intrusion Detection Algorithm - A deep learning system, storing data on a separate chain to identify malicious nodes through behavioral feedback.

Isolated - Isolation of third-party code is key to maintaining network integrity and performance and is a core feature of Smart Contracts.

Leader node - A leader node is selected every 60 seconds, entirely at random via the LSA, to confirm transactions during that period, until a new leader node is selected and it returns to its original node status.

Leader Selection Algorithm (LSA) - The leader selection algorithm uses a three-phase process, that makes use of the NIST integration, to choose the next leader node to process transactions for the next 60 seconds:

- **Resource evaluation: Assessing the suitability of a node to process transactions including available bandwidth, CPU and flag trust via the PIP.**
- **Leader selection: A random quorum of nodes are selected from the NPD to confirm/reject blocks for the interval.**
- **Block confirmation: Submitted blocks will then be validated before addition to the blockchain.**

Merkle tree - A Merkle tree is a hash-based data structure that is a generalization of the hash list. It is a tree structure in which each leaf node is a hash of a block of data, and each non-leaf node is a hash of its children. Typically, Merkle trees have a branching factor of 2, meaning that each node has up to 2 children.

Mining - Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger of past transactions. Miners use special software to solve math's problems and are issued a certain number of bitcoins in exchange.

NIST Randomness Beacon - The Beacon is a source of truly random numbers generated by light photons, that broadcasts full-entropy bit-strings in blocks of 512 bits every 60 seconds, providing three key functions; unpredictability, autonomy, and consistency.

Nodes - A node maintains a copy of a blockchain and can participate in confirming transactions.

Node announcement - Every node joining the temtum network must announce itself to an authority node with information such as public key and ip-address.

Node descriptor format - The descriptor is a summary of the node, including its nickname, IP address, bandwidth and uptime.

Node Participation Document (NPD) - The Node Participation Document stores the latest details of all network nodes, with every node holding the latest copy to query when required. The NPD is maintained by Authority Nodes.

Nonce - An arbitrary number that can be used just once in a cryptographic communication.

Optimized Routing Algorithm (ORA) - An alternative to existing 'gossip protocols' apparent in existing blockchain network, temtum's ORA ensures efficient routing of transactions by only sending to the block leader, the Leader Node.

Peer-to-peer - A process where two parties communicate in the sharing of data, files, goods or in the case of cryptocurrencies, transactions, without a central authority.

Performance Integrity Protocol (PIP) - The PIP assesses the performance of nodes as an internal reputation management system, requiring up time, resources and trusted performance over a period of time to be selectable as a leader node or remain included in the NPD.

Private key - A generated string that grants access to a specific wallet and must be kept secure. Used to generate a public address.

Proof-of-stake - A consensus algorithm where crypto assets are staked to maintain a network, with rewards distributed in return - much like a loan.

Proof-of-work - The most widely used consensus algorithm that rewards the solving of complex equations (Mining) to incentivize a network for processing power and electricity consumed.

Public address - A cryptographic hash of a private key, public addresses are used as locations for data and transactions to be sent to.

Quantum randomness - Quantum randomness doesn't utilize any software and ensures genuine random number generation, which is significantly more secure than software generated, pseudo-random number generators.

Smart contract - Transactional rules constructed in code and enforced by the contributing network to remove the need for a central authority any given action.

Sybil attack - Also known as a 51% attack where a malicious entity can control a peer to peer network by flooding the network with artificial peers or nodes directly controlled by the attacker.

Temporal Blockchain - The evolutionary peer to peer network that forms the technological foundations of the temtum cryptocurrency, as a genuine next-generation blockchain platform.

Temporal node - A Temporal node is a standard contributing node to the Temporal Blockchain and features on the NPD.

Terminable - In order to ensure a process can, complete in a set time, it may also need to be terminated to prevent a never ending loop that will not be efficient. A core feature of smart contracts.

Tokens

- **Utility token – that provide access to a service.**
- **Security token (or asset coin) – that represent rights in or to assets or businesses.**

TPS – Transactions per second.

TXO – Transaction output.

UTXO – Unspent transaction output.

Wallet - A wallet refers to a secure cryptocurrency store of assets, maintained with a user's unique public and private key pair.

Community

Email - info@temtum.com

Reddit - r/temtum

WWW

Website - temtum.com

Telegram - t.me/temtumofficial

Facebook - @wearetemtum

YouTube - @temtum

Twitter - @wearetemtum

Medium - @temtum

Discord - @temtum

GitHub - /temtum

temtum

Cryptocurrency. Evolved.