GRAHAMBELL

Introductory_Whitepaper_v0.1 _November2025_Version_Pakistan
Chapter 1

Descaling and Controlling Proof of Work (PoW) mining speeds to 1 Hash per second per hardware (1H/s/hw)

Mine Blocks During an Audio or Video Call

1 CPU = 1 Vote Ideology

The Next Chapter of CPU Mining (Phone = PC = ASIC)

ASIC PROOF SOLUTION

Blockchain 1.0 x Telecommunications 2.0

By: Hurairah Shamsi (Abu Hurairah Zeeshan)
hurairah@grahambell.io

Table of Contents

Legal Disclaimer

This document is for informational purposes only and does not constitute investment, legal, or financial advice. The GrahamBell project is in its early stages, and all details provided herein are subject to change as development progresses. We make no warranties, express or implied, regarding the accuracy, completeness, or future performance of the information contained in this paper.

Participation in blockchain and cryptocurrency projects inherently involves risks, including but not limited to regulatory changes, technological failures, market volatility, and security vulnerabilities. The regulatory environment surrounding blockchain and cryptocurrency is evolving, and the implications of such changes may impact the project and its users. GrahamBell makes no representations or guarantees about compliance with any specific legal or regulatory requirements and strongly advises participants to stay informed of relevant changes in their jurisdiction.

GrahamBell does not guarantee any specific returns, outcomes, or benefits from the use, mining, or participation in the ecosystem. All participants acknowledge and accept the risks associated with engaging in such projects. Before making any decisions related to GrahamBell, prospective users, investors, and contributors should conduct their own due diligence and consult with qualified legal, financial, and technical advisors.

By engaging with the GrahamBell ecosystem, participants release GrahamBell, its affiliates, and team members from any liability, claims, or damages arising directly or indirectly from the use, interpretation, or reliance on the information presented in this document or any associated activities. This paper does not constitute an offer to sell, nor a solicitation to buy, any securities, financial instruments, or other regulated products.

All participants are solely responsible for securing their assets and understanding the risks related to blockchain and cryptocurrency technologies, including but not limited to risks associated with network disruptions, software bugs, or security breaches. GrahamBell disclaims any responsibility for losses due to individual failures in security or technical understanding.

Furthermore, this paper is not intended to target or critique any existing mining pools, blockchain or telecommunications systems. It is designed to highlight industry-wide challenges and explore potential solutions that may enhance decentralisation, security, scalability and accessibility in the long run. The ideas and concepts presented are meant to foster innovation and collaboration rather than to directly compete with or undermine any existing technologies or entities.

By reading this document, you agree to release and hold harmless; GrahamBell, its team members, and affiliates from any claims, liabilities, or damages resulting from the use or interpretation of the information provided herein and from the participation in the GrahamBell ecosystem.

Abstract:

GrahamBell proposes a fair-mining Proof-of-Work (PoW) ecosystem where all devices mine at 1H/s (per hardware), enforced by a decentralised layer called Proof of Witness (PoWit). Combined with Witness Chains (WCs) for network integrity, GrahamBell ensures equality, fairness, accessibility, and environmental sustainability. Additionally, a unique system Proof of Call (PoCall) is a novel mechanism that links mining with telecommunications activity.

The concept aims to restore the original promise of **"1 CPU = 1 Vote",** eliminating ASIC dominance, mining pools, and centralised communication infrastructures and introduce a new system where mining occurs during audio/video calls.

***Note:** This document intentionally omits internal protocol details for intellectual property protection. The purpose of this Introductory Whitepaper is to introduce the concepts and architecture at a high level. Full technical specifications for each protocol (PoWit, PoCall, WCs, etc.) will be released in phases aligned with their testnet deployment.*

Introduction

Telecommunications revolutionised global connectivity, enabling seamless audio and video communication that fuels business growth, access to information, education, and economic expansion, becoming an essential part of daily life. Similarly, blockchain technology, pioneered by the unknown Satoshi Nakamoto, is still in its early stages but holds immense potential to transform digital trust, decentralisation, and security—especially in finance and contracts.

Despite rapid advancements, both industries face critical challenges:

- Blockchain struggles with mining pool dominance, centralisation, low scalability, high storage costs, energy inefficiency, and unfair mining accessibility, making it unaffordable for average users to host a solo setup and compete independently within the network. These core issues have led to a lack of mass adoption, decentralisation failures and security vulnerabilities in existing blockchain systems.
- Telecommunications lacks security, decentralisation, and interoperability. Users rely on centralised third-party entities that control communication networks. Even companies that claim to provide end-to-end encryption for using their services can often access user data, raising significant data privacy and security concerns.

Overview

Around 80% of Bitcoin's hash-power is concentrated among eight mining pools (source: Hashrate Index, snapshot Nov 2025), and the global market for ASIC mining hardware was valued at over US $15 billion as of 2025 (source: Valuates Reports, 2024 ASIC Bitcoin Mining Hardware Market Report).

GrahamBell brings a new chapter of blockchain and telecommunications innovation, redefining Proof of Work (PoW) mining through novel consensus mechanisms and architectural breakthroughs.

It descales and controls the computational power requirements, reducing mining power to as low as 1 hash per second per hardware (1H/s/hw) without any centralised control (preventing vertical scaling). Additionally, the system also limits the number of independent active mining hardware per registered node ID to ensure a minimum of 1 mining hardware operates per node ID within the network (limiting horizontal scaling). Unlike traditional PoW mining, which favours expensive ASICs and GPUs, GrahamBell's model ensures fair, equitable and environmentally friendly CPU mining, encouraging mass adoption which in return would assist with optimal security, true decentralisation, and industrial scalability. This design ensures the computational power of **1 PHONE = 1 PC = 1 ASIC**, meaning every device from low end phones to high-end ASICs mine at the exact same speed.

Furthermore, GrahamBell integrates telecommunications with blockchain consensus, ensuring Proof of Work (PoW) blocks are only mined during audio or video calls. This innovative approach not only fosters the development of interoperable, open-source, and decentralised communication platforms but also enhances security, user control, and independence from centralised telecom service providers.

By linking mining incentives to widely adopted real world communications activities, GrahamBell drives mass adoption (encouraging new miner/node registration), ultimately strengthening security, decentralisation and scalability within our ecosystem.

Problems in Blockchain

Mining Pool Dominance:
Mining pools emerged as a solution to the problem where individuals could scale their hardware both vertically and horizontally by purchasing expensive, high-performance hardware. This created a situation where only those who could afford such setups were able to compete, leaving those with slower, cheaper hardware at a disadvantage. To address this disparity, mining pools were introduced, allowing people to make smaller investments and earn proportional returns based on their contribution (i.e., a small group of individuals make small contributions to stake together to host a validator or buy expensive hardware collectively to mine a Proof of Work currency by connecting to a mining pool). However, as mining pools scale to meet growing demand, they often compromise decentralisation and security. Additionally, mining pools enable users to connect their infrastructure across different geographical locations, with the pool allocating tasks to the connected hardware and distributing rewards upon completion. While this mining pool model makes participation in mining more accessible, it consolidates computing power, shifting control into the hands of a few players and potentially leading to centralisation. This goes against the fundamental decentralised principles of blockchain technology.
Problems:

- A few dominant mining pools control the majority of the network's hash power, leading to centralisation of the network.
- Pools can collude with each other to manipulate the network, compromising the integrity of the blockchain.
- Mining pools have the ability to censor transactions (include/exclude them), undermining the principles of censorship resistance.

- Government pressure on mining pools within their jurisdiction can lead to the censorship of transactions, as seen with Marathon Digital Holdings, which began censoring transactions that did not comply with U.S. regulations.
- Governments can regulate or shut down mining pools within their jurisdiction. E.g., China imposed a nationwide ban on mining in 2021, driving miners out of the country. Miners can join other pools in distinct geographical regions, but they may face higher latency and lower chances of earning rewards compared to those in favourable jurisdictions.
- The dominance of large pools makes solo mining impossible due to the extreme difficulty level and lack of rewards which is important to promote decentralisation and security.
- By sending pre-hashed previous block hashes (the hashed version of the hash of the previous valid block) and block numbers, mining pools can take away a hashing step from the miners. This can allow them to hide the block they are making the miners mine, enabling them to manipulate mining and potentially re-mine earlier blocks, increasing the risk of double-spending or rewriting the chain. While the miners using a node can hash previous valid hashes of the longest chain and confirm which block the pool is making them mine, it would still be useless considering the pools have the final say.
- Switching pools can increase latency due to geographical distances between miners and pools, reducing mining efficiency, which can also cause unintentional withholding attacks. One would also consider switching pools based on profitability; if it is not profitable, miners simply would not switch.
- There is a potential risk that pool operators may steal pay-outs, especially if they are dishonest or lack transparency.
- Mining pools are often centralised constructors of block templates, using super nodes and super mempools. This leads to a situation where miners deal directly with pools and often ignore the broader network of mempools or host their own nodes.
- They can sell block space for higher transaction fees, which could prioritise profit over the health and integrity of the network.
- Mining pools can be dishonest or choose not to be transparent with their practices, reducing trust.
- The majority of miners choose FPPS (Full Pay Per Share) because it offers a reliable, stable, predictable, and guaranteed income based on the computational power they contribute, rather than the actual blocks they help mine, which is appealing. However, this model comes with significant trade-offs:
    - Miners give up control over the block content, increasing the risk of potential manipulation and loss of funds.
    - The lack of visibility into block content makes it difficult to verify pool operators' practices and reward distribution.
    - Pool operators can manipulate the pay-out structure or hide transaction fees, leading to dishonest behaviour.
    - Since miners are rewarded based on their hash rate rather than the actual blocks they mine, the majority of participants, many of whom are non-technical users, tend to focus primarily on earning income. As a result, they do not care or tend to lose interest in the legitimacy of block contents or the overall health of the network, which undermines the security and integrity of the network.
- Mining pools can appear to have less hash power publicly while secretly redirecting hash power from smaller pools with or without smaller pool operators knowing (e.g.,

bribing miners connected to small pools with a greater profit share or colluding with small pool operators), allowing them to maintain control over a larger share of the network. This hidden manipulation makes it harder to detect unfair practices, like block withholding attacks, where miners withhold valid blocks to harm smaller pools or disrupt the network.

- Miners (hashers) often prefer to join larger mining pools because they offer a higher likelihood of profitable payouts due to their larger hash power. Smaller pools, on the other hand, are more vulnerable to attacks like block withholding, where malicious miners withhold blocks, making it appear as though the pool is underperforming. This harms honest miners in smaller pools by reducing payouts. However, the downside of joining larger pools is that they concentrate hash power, which could threaten the decentralisation and security of the blockchain, as a few large pools might exert too much control over the network.
    - Larger pools can also intentionally target smaller pools connected with them by secretly redirecting their hash power to smaller pools for withholding attacks to gain optimum control of the network. They can propagate the block with a delay, causing small pool operators to believe it was a network delay rather than an intentional delay or make miners connected to a small pool withhold valid blocks.

Stratum V2

Stratum V2 is a significant step towards increasing decentralisation and security in a network. It grants miners more autonomy by allowing them to propose their own block templates, reducing mining pool dominance over transaction selection. However, there are notable drawbacks. After all, the pool still has the final say in the entire process.

Template Validation Load & Template Providers

- If a mining pool is connected to a large number of miners, and each miner proposes a different block template, the pool would face an overwhelming validation burden, leading to potential delays in block propagation.

Proposed Solution:

- Template Providers: Stratum V2 introduces template providers, which provide a single block template for a collective group of miners, reducing computational overhead for the pool. Mining farms or individual miners can act as template providers for others.

Problem:

- While this improves efficiency by reducing validation time for the pool, it also introduces centralisation risks:
    - Large template providers could dominate the network by having a disproportionate influence over block template proposals, leading to transaction censorship or prioritisation, or potentially allowing pools to collude with template providers.
    - Mining farms could coordinate to control which transactions are included in blocks, reducing miner autonomy.
    - Since template providers are not yet widely adopted, pools might set up their own private template providers rather than allow external ones to influence pools.
    - In the end, the decision and control belong to the pools, who get to decide which templates to accept or reject as proposed by the miners, who may even choose to have their own custom templates to be mined by all connected miners.

This means pools can secretly use their own templates without losing control. However, they can prioritise transactions proposed by miners for profit and subtly manipulate transaction inclusion or block templates.

Pools Prefer Trusted Sources

- Mining pools tend to prefer block templates from trusted sources, such as miners with a higher hash rate, to ensure stability and reduce the risk of invalid blocks. Additionally, pools often implement rate-limiting measures, restricting the number of templates accepted per epoch to prevent spam and/or performance issues.

Problem:

- Larger miners or trusted sources gain a dominant advantage, leading to a system where smaller miners have less influence over block selection, further concentrating power amongst larger miners. This is because trusted sources and larger miners may optimise profitability and efficiency for the pool.
- Smaller miners, who can propose templates, may struggle to have their templates accepted (i.e., low acceptance rate), discouraging and limiting participation in transaction selection and reducing overall decentralisation.

Single Template Acceptance by the Pool

- Ultimately, even with Stratum V2, the mining pool has the ability to select and accept a single block template, initially proposed by the connected miners, and forward it to all miners within the pool.

Problem:

- Collusion risk: A pool could collude with a template provider or could secretly generate its own block template while falsely claiming it came from a random miner, effectively manipulating the transaction selection process, introducing the following issues:
    - Censorship risk: If a mining pool decides to exclude specific transactions (e.g., due to government regulation or private incentives), miners in that pool would have no control over it.
        - If multiple large mining pools implement censorship policies (e.g., excluding transactions flagged by governments), then miners inside those pools have no way to resist, reinforcing the risk, which may not even be prevented by switching pools under the same government influence.
    - Selling block space: Mining pools could prioritise high-fee transactions or offer exclusive deals to certain users, undermining fairness.

Ultimately, it would lead to a lack of transparency and undermine trust in the process.

Mining Pools Are Businesses – Profit Over Decentralisation?

- While Stratum V2 allows miners to propose block templates, mining pools still have financial incentives to optimise for efficiency rather than true decentralisation and security.

Problem:

- If improving decentralisation increases costs (i.e., infrastructure to handle the increased load of independent template validation), pools may choose to prioritise profitability over miner autonomy.
- Pools with better infrastructure could dominate, further concentrating power.

Ending Statement:
Stratum V2 is a step in the right direction for decentralisation, but it does not completely eliminate centralisation and security risks. Since pools ultimately decide which templates to accept, collusion, censorship, and profit-driven behaviour remain real concerns.

In the end, this means that true miner independence still requires additional innovations beyond Stratum V2 to ensure that pools do not become the hidden centralised gatekeepers of blockchain transactions.

Energy Inefficiency and Environmental Damage

- Proof of Work (PoW) mining requires substantial computational effort to solve cryptographic puzzles, which results in very high energy consumption. Modern PoW networks are dominated by specialised ASIC hardware, which continually escalates the overall network difficulty. Since only one miner can receive the reward for each valid block, the vast majority of this energy expenditure effectively becomes wasted from an efficiency perspective. Although, in theory, transitioning to lower-power hardware (such as CPUs or GPUs) could reduce the environmental impact, **economic incentives** naturally drive miners to maximise their computational capacity. As long as increased hash power correlates with a higher probability of earning block rewards, miners are encouraged to scale their operations both vertically and horizontally. This behaviour consistently reinforces reliance on high-performance, energy-intensive hardware.Today, the total electricity consumption of large PoW networks exceeds that of entire countries—including Pakistan, Argentina, the Philippines, and the United Arab Emirates—placing a measurable burden on the environment. A study by the United Nations University (UNU) estimated that offsetting Bitcoin's annual carbon footprint would require the planting of nearly 3.9 billion trees. While the use of renewable energy is often proposed as a solution, this does not fully address the structural problems. Renewable-only mining remains unaffordable for most users, encourages industrial-scale setups, and continues to incentivise the formation of mining pools. These effects ultimately reduce decentralisation and exclude the average participant, preventing the broad-based mass adoption necessary for optimal network security.

Unaffordability, Unfairness, Inequality and Lack of Mass Adoption

- In a decentralised network where users have the freedom to use any hardware they want and add as many devices as they can afford in the network, then without an established system to track the number of active concurrent devices or the hash rate per second for each piece of hardware online, users can scale their mining operations in two ways. First, they can scale vertically by adding more processing power to a single machine, making it as fast as possible. Second, they can scale horizontally by adding more vertically scaled machines, essentially expanding their mining rigs. This is because, in a decentralised environment, such control mechanisms do not exist; implementing them would require adding control in an area where control is intentionally limited. Without a way for the network to track or control the number of devices owned by a single user, this scaling process can potentially lead to users gaining disproportionate control of the network. This dynamic leads to centralisation trends and economic barriers that limit broad participation (i.e. moving towards expensive hardware), which in turn reduces the likelihood of widespread network adoption—something that is key for optimal security and decentralisation.

- Fee sniping or fee bumping is a problem where miners re-select transactions, replacing initially added transactions with newer ones because of a higher fee attached to them, resulting in greater profit for the miner. This results in:
    - Unfairness for the original user who submitted the transaction with a reasonable fee, meaning they would have to wait longer or resubmit their transaction with a higher fee, essentially being extorted.
    - Instability in the network by putting pressure on users to overpay higher fees just to avoid being sniped, leading to unpredictable and inflated fee rates within the network.
    - Congestion in the network because miners would naturally prioritise transactions with higher fees for higher profits, leaving lower-fee transactions stuck in the mempool for extended periods.

Incentive-Driven Upgrades

- Since blockchain operates as a trustless system, where participants do not need to trust each other for data processing and validation, honest participants are naturally motivated to keep their hardware up to date, automatically scaling the network hash rate. This occurs with little concern for environmental harm and energy consumption, as long as mining remains profitable. However, if honest miners choose not to upgrade their hardware, promoting CPU mining, which makes the system fair, affordable, and accessible for all, malicious participants can exploit this gap by investing more in powerful hardware, potentially gaining control of the network's hash rate. Since there are no inherent restrictions on hardware accessibility, both malicious and honest miners are incentivised to continuously upgrade their equipment, either to secure and protect the network's integrity or target it. This is why existing Proof of Work (PoW) chains are generally not inclined to descale computational resources, as doing so could compromise the security and integrity of the network even if honest participants are willing to descale.

Scalability

- On-chain scalability is a major issue for blockchain systems, primarily due to storage requirements. All blockchains must store significant amounts of ledger data, which can lead to centralisation, as node operators are required to continually upgrade their hardware to accommodate growing storage needs. Hence, increasing Throughput Per Second (TPS) significantly requires substantial storage, which is costly and can lead to centralisation and low security, as not everyone will be able to afford to host a node/validator.
- Sharding is one solution to solving the storage problem associated with scalability, but it also introduces centralisation risks. In sharded blockchains, the beacon chain is ultimately responsible for storing data from all sub-chains (shards). As a result, only a few individuals with the necessary resources (i.e., expensive hardware, storage requirements) can afford to run validators or nodes on the beacon chain. Additionally, the high staking requirements to become a validator in the beacon chain also leads to centralisation, as only a small number of participants can afford to take part, potentially leading to a **51% takeover**. This centralisation can introduce vulnerabilities in consensus, as a small group of nodes controlling the beacon chain could potentially lead to a **51% attack**, allowing an attacker to manipulate the ledger. Cross-shard communication, such as transferring tokens between shards, presents its own challenges, such as delays or vulnerabilities. While it's a smaller issue than storage, mistakes like mismanagement, errors, and incorrect shard IDs during token transfers

can result in the permanent loss of funds, further complicating the system. Furthermore, scalability with sharding also has limitations, such as the number of shards that can be effectively managed and coordinated at a time.

Proof of Stake (PoS)

- Expensive to host independently due to the staking requirements.
- Staking pools can be created, which leads to centralisation. Although this increases staking accessibility for small holders, it gives control to pool operators in making consensus and governance decisions.
- The design of a Proof of Stake system, along with the staking requirement to host an independent node, gives a significant unintentional advantage to those who already hold a large amount of the corresponding native currency. This means that the more an individual stakes, the higher their chances are of becoming a frequent block proposer. This leads to immense power and influence being concentrated in the hands of a few large stakeholders within the network, with significant influence over governance decisions, which is far from promoting fairness.
- Large stakeholders can collude and gain control over the network, influencing governance decisions, which is also far from promoting fairness.
- Entities that hold large reserves of fiat currency or any widely adopted cryptocurrency can offer attractive deals to users, such as: "Deposit your native Proof of Stake currency with us, and we will give you liquid capital (fiat or another cryptocurrency) in return." They can also create an independent currency, referred to as "pool currency," designed solely to provide users with an equivalent amount in exchange for the native currency deposited for staking. Staking rewards are then paid back to users in the form of fiat currency or other widely used cryptocurrencies, rather than the native currency. This practice serves to increase the entity's reserve of the native PoS currency. As a result, these entities can buy influence over the network, undermining security and leading to centralisation. With vast control over the native currency, they can exert significant influence on network governance. Although stakers have not sold their native currency, the attention-grabbing deals allow these entities to vote on protocol upgrades, changes to the reward system, and other key decisions—often benefiting themselves at the expense of other network participants. This creates a powerful incentive for users to delegate their staking power to these entities. Furthermore, by offering incentivised deals, these entities influence users' decisions to choose them for staking, leading to further centralisation without requiring specialised hardware or technical expertise on the user's end.
- Governments around the world are still figuring out how to regulate cryptocurrency staking, and this uncertainty is a big problem for networks that use Proof-of-Stake (PoS). If staking is to be classified as a security, similar to stocks, it will make things much harder and more expensive for PoS networks to operate. This could hurt innovation and participation, making it harder for regular people to participate, and lead to more control by large companies, resulting in centralisation. Furthermore, varying regulations across countries adds another layer of complexity because different countries have different rules, which can make things complicated for projects that want to work globally. Essentially, this regulatory uncertainty is a major roadblock for the growth and potential of PoS technology and could lead to unforeseen consequences.

Blockchain Problems Ending Statement:
The issues highlighted above regarding the core principles of blockchain have led to a lack of mass adoption, decentralisation failures and security vulnerabilities in existing blockchain systems, which are crucial for the success of any blockchain infrastructure.

Problems in Telecommunications

Security and Centralisation

- Existing communication platforms (VoIP, messaging, video calls) rely on centralised providers, which raises privacy concerns and issues of control. Despite claims of end-to-end encryption and secure services, these platforms can still access user data, compromising data privacy and raising significant security concerns.
- Many existing communication platforms may be selling your data without your consent, profiting from your personal information without your knowledge.

No interoperability

- The lack of interoperability between communication platforms like WhatsApp, FaceTime, and others creates significant barriers, particularly in regions where these services are restricted or less commonly used. For example, services like WhatsApp and FaceTime are inaccessible in countries like China and certain Gulf regions. As a result, users are forced to rely on region-specific alternatives like WeChat or BOTIM. This fragmentation leads to a disconnected communication experience, making it difficult for users to connect easily across platforms, reducing convenience and potentially hindering collaboration.
- Interoperability is essential for fostering healthy competition because it prevents any single platform or service provider from locking users into their ecosystem. Without cross-platform communication, users are more likely to stick with one service, limiting their options and making it harder for competitors to grow. This lack of competition diminishes the incentive for innovation, as providers face less pressure to improve or offer new features. Open communication between platforms encourages innovation and ensures that users continue to benefit from better, more diverse services over time.

Not Open-source or Decentralised

- Not making the communications sector decentralised and opensource takes away a significant important page of potential innovation, including:
  - **Increased Accessibility:** Open-source solutions provide free access to code, making communication tools more affordable and accessible to underserved communities or regions where communication tools are expensive.
  - **Enhanced Security and Privacy:** Decentralisation and open-source code would strengthen privacy and security. It would make it harder for third parties to monitor communications and enable public security audits to identify and address potential vulnerabilities.
  - **Greater Transparency:** Open-source platforms would offer greater transparency, allowing users to understand how their data is handled. It would ensure that security measures are visible and auditable, fostering trust and accountability—something that is often lacking and harder to achieve in closed-source software.

- **Reduced Centralisation Risks:** Decentralisation would reduces the risk of a single entity controlling the communication infrastructure, making systems more resilient to censorship, manipulation, and outages—issues common in centrally controlled systems.
- **Fostered Innovation:** Open-source development would encourage community collaboration, leading to faster innovation and continuous improvements in features and functionality.
- **Improved Interoperability:** Open-source platforms can follow open standards, enhancing connectivity and breaking down barriers between different communication systems, making it easier for users to communicate across platforms.
- **Increased Customisation:** Open-source systems would allow users to modify the platform to suit their specific needs, offering greater flexibility that proprietary systems (third-party) cannot provide.
- **Community Ownership:** Open-source projects are community-driven, giving users a say in the platform's direction and development, further encouraging innovation.
- **Resilience to Disruption:** Decentralised systems are more resilient to disruptions since they do not have to rely on a single point of failure, unlike centralised infrastructures.
- **Lower Costs:** Open-source solutions eliminate licensing fees, making communication tools more affordable for both individuals and organisations.

Solution (GRAHAMBELL)

Proof of Witness (PoWit): Decentralised, Fair, Equitable and Affordable Mining

- Ensures consensus for events.
- Ensures consensus for computational power/hash rate.
- A layer that operates in parallel with the Proof of Work (PoW) layer.
- A system designed to descale and control Proof of Work (PoW) computational power without any centralised control, setting the same hash rate allowance for all miners, promoting fairness and equality.
- A novel infrastructure designed to only allow CPU hardware speeds to mine a Proof of Work (PoW) block, promoting accessibility.
- Environmentally friendly mining compared to other blockchain systems.
- Eliminates ASIC/GPU mining dominance, enabling true decentralisation.
- Encourages mass adoption by making mining more accessible.
- Helps prevent the formation of mining pools.
- Enables mining to be energy-efficient and environmentally friendly.
- Assists in making the hosting infrastructure and mining more accessible and affordable for the average user.
- Assists in optimising security and decentralisation of the network by encouraging individuals to host, again promoting mass adoption.
- Requires Witness Chains (WCs) to operate.

Proof of Call (PoCall): Secure & Decentralised Communication: Mine during calls

- An extension of Proof of Witness (PoWit).

- A layer that operates in parallel with the Proof of Work and Proof of Witness (PoWit) layers.
- Enables the integration of audio/video calls with blockchain consensus, ensuring blocks are only mined during an audio or video call.
- Ensures consensus for audio/video calls.
  - Miners can be in a call or a call room without requiring another user on the call with them to mine blocks.
- Encourages the development of open-source and decentralised telecommunications platforms to be integrated with blockchain consensus in order to propose blocks.
  - Develop and host your own independent calling platform/services and calling servers, e.g., STUN, TURN, Signalling, SFU, MCU, and more, geographically cascade them to ensure global connectivity.
- This mechanism removes the need for third-party communication services, significantly reducing surveillance and censorship risks in global communications.
- Significantly enhances security, privacy, and decentralisation through open-source and decentralised telecommunication developments.
- Requires Witness Chains (WCs) and Proof of Witness (PoWit) to operate.

Registration: Protecting network integrity, limiting horizontal scaling and denying the formation of mining pools

- Miners must be registered with a valid node ID following the registration mechanism to propose a block to update the ledger.
- If an unregistered miner proposes a transaction block, the network will reject it, even if the block contains valid data and has a valid Proof of Work (PoW) hash.
- Unregistered miners are allowed to propose a registration block to form a valid node ID.
- The registration block proposed by an unregistered miner will be accepted by the entire network if it is considered valid.
- The hash of the registration block will be considered the registered node identity within the network.
- The registration of a valid node ID, along with other necessary information, greatly assists in limiting the horizontal scaling of the network by allowing only one active miner per registered node ID that can mine at any given time. Additionally, sub-node IDs can be proposed and registered after specific epoch intervals, with each sub-node ID requiring an independent node setup for additional devices, allowing one mining hardware to operate concurrently per sub-node ID. The maximum number of sub-node IDs per registered node ID is capped at four, meaning a single registered node ID can have a total of five active miners mining concurrently within the network—one for the node ID and four for its sub-node IDs. This ensures controlled hardware scalability within the network without any centralised control.
- It helps make the system Sybil-resistant.
- It helps blacklist malicious node IDs from the network, preventing the malicious actor of that node ID from proposing blocks in the future, thereby protecting the overall integrity of the network.
- Registration (valid node IDs) will also assist with node allocations within the network.

Witness Chains (WCs): Backbone to Descale and Control Computational Power and Enhance Transaction Scalability.

Descaling: balancing and capping of computational output across nodes to ensure fair participation, regardless of hardware capacity.

- Witness Chains (WCs) = Decentralised Monitoring Servers (DMS).
- Enables consensus for events.
- Witness Chain (WC) consensus is the underlying and crucial infrastructure to enable consensus for Proof of Witness (PoWit) and Proof of Call (PoCall).
- Designed to add decentralised control in a decentralised system.
- Witness Chain (WC) members will be incentivised for witnessing nodes and miners honestly. Hence, Witness Chain servers/nodes must remain online.
- A decentralised system where witness nodes/servers monitor and witness other Witness Chain servers/nodes and miners for the security and integrity of the network. They will not benefit if they collude with each other to act maliciously, but will be significantly harmed if they collude dishonestly. This means their chances of being incentivised would drop to zero, or even below zero for miners, costing them out of pocket for dishonest behaviour. This encourages every Witness Chain member and miner to act honestly and follow the rules.
- Assists in limiting horizontal scaling per node ID, along with registration.
- Allows the network to set the same computational power threshold for each miner to as low as 1 hash per second per hardware (1H/s/hw), 1 hash per hour per hardware (1H/h/hw), 1 hash per 24 hours per hardware (1H/24hr/hw), or even lower.
- Assures that every miner stays within the agreed network hash rate threshold, completely preventing vertical scaling of hardware per node ID.
- Plays a major role in blacklisting malicious node IDs permanently from the network.
- Ensures Proof of Work (PoW) blocks are only mined during an audio or video call.
- The Witness Chain (WC) will have a witness cap (the number of miners it can witness concurrently) and a request cap (the number of concurrent requests it can handle). The request limit will be variable and dynamically adjusted based on the remaining capacity to witness total miners concurrently per WC, preventing overloads and mitigating DoS (Denial of Service), DDoS (Distributed Denial of Service), and unintentional DDoS attacks.
- Prevents miners from recalculating previously confirmed blocks within the network.
- Significantly resists miners from continuously re-ordering transactions and re-selecting different transactions from the same block upon realising that transactions with higher fee opportunities are available, which were previously unavailable at the time of computing the Merkle root (i.e., fee sniping).
- Ensures transactions can only be reordered and re-selected from a block if the corresponding block number is updated to a newer one (n+1), promoting a first-come, first-served paradigm in transaction selection.
- Assists in preventing the formation of mining pools.
- Enables mining to be energy-efficient and environmentally friendly.
- Assists in making the hosting infrastructure and mining more accessible and affordable for the average user.
- Contributes to the optimisation of security and decentralisation of the network by encouraging individuals to host - ensuring fair participation - and promoting mass

adoption, which in turn helps increase scalability through the Single Chain Architecture (SCA).

Scalability: Single Chain Architecture (SCA)

- Multiple Data Saving Groups/Servers (DSG/S) will assist in significantly reducing the ledger storage requirement per node per year.
- Designed to achieve industrial scalability using a Single Chain Architecture (SCA), meaning the entire network can participate in consensus, regardless of whether the data is partitioned across multiple Data Saving Servers/Groups.
- Proof of Funds (PoF) and the Proof of Funds (PoF) Hash Table will aid the network in fast block acceptance and validation, without requiring each node within the network to store the entire history of the ledger. This allows every node, across all groups/servers, to participate in block acceptance and validation.
- Very Last Latest Block/Very Last Latest State (VLLB/VLLS) is designed to validate newly fast-accepted/validated blocks before their maturity (confirmation) time, in case of any malicious activity.
- The Pyramid System (TPS) is designed to enable fast block propagation across the entire network.
- The Block Processing Unit (BPU) and Block Validation Unit (BVU) will assist in validating and processing data, contract code, and Merkle roots in parallel, using multiple available cores efficiently.
- Proof of Recognition (PoRcg) will ensure that each node under a Data Saving Group is storing the necessary data (ledger history) allocated for that specific DSG/S.
- This infrastructure ensures that throughput per second (TPS) continuously increases as mass adoption of nodes grows within the network, without affecting storage requirements. These requirements will increase by the same amount each year and remain extremely low for each. However, storage for the PoF hash table will vary, gradually increasing or decreasing over time depending on user adoption. This growth occurs when a wallet contains an active balance and/or a transaction counter within the network. Therefore, the gradual increase in PoF hash table storage is proportional to the number of wallet addresses with an active balance and/or a history of the transaction counter (i.e., the number of transactions made or received). Storage requirement can also decrease, if a wallet that previously had a positive balance is reduced to a zero balance. As a result, the yearly storage requirement for the PoF hash table for nodes would remain extremely low.

Chain Allocation Committee (CAC): Node and Server Allocations

- Ensure the validity of newly registered node IDs by validating their registration blocks.
- A system design that continuously updates the committee, replacing existing CAC members with new and randomly elected nodes from the entire infrastructure, thus protecting the integrity of the network.
- Designed to reach a consensus among the committee members to allocate unallocated or newly registered nodes to existing or newly formed Witness Chains (WCs) and Data Saving Groups/Servers (DSG/S), using a degree of randomness.
- Designed to form new or delete existing Witness Chains (WCs) and Data Saving Groups/Servers (DSG/S), depending on the adoption rate of the network.

- Will help the network by reducing the likelihood of a 51% takeover in Witness Chains (WCs) and Data Saving Groups/Servers (DSG/S).

Murphy: Reverse Billing Infrastructure

- Independent of the blockchain and in addition to decentralised block rewards, Murphy is a centralised reward system designed to provide additional incentives for network participants during audio/video calls.
- Rewards are distributed on a per-second basis during audio/video calls to both individuals with registered nodes and unregistered users for their participation in calls.
- Individuals with active, running registered nodes in the network will receive a higher reward, while unregistered users will receive a lower reward comparatively, on a per-second basis during calls, encouraging users to get a node registered within the network and actively run it, promoting mass adoption, which significantly contributes to network security, decentralisation and scalability.

Next Steps, Opportunities, and Community Building

GrahamBell welcomes contributors across engineering, research, security, telecommunications, and community roles. As the project progresses toward its P2P testnet phase, early collaborators will have the opportunity to contribute to development, testing, feedback, and real-world implementation of the architecture.

Who is behind GrahamBell?

- Abu Hurairah Zeeshan (Hurairah Shamsi) = Founder and Inventor of GrahamBell, Theoretical Protocol Solutions Engineer, Architect and Researcher

Ecosystem Links

Website: https://grahambell.io/

Twitter/X: https://x.com/gbellofficial

Facebook: https://www.facebook.com/GrahambellOfficial

Instagram: https://www.instagram.com/gbellofficial/

LinkedIn: https://www.linkedin.com/company/grahambell

Reddit: https://www.reddit.com/r/GrahamBell/

GitHub: https://github.com/gbellofficial

Contact us:

General Queries
Info@grahambell.io

Key Takeaways

• **1H/s per device** → hardware fairness and affordable participation
• **Witness Chains** → decentralised enforcement
• **Proof of Call** → mining during audio/video calls
• **Single Chain** Architecture → scalable infrastructure
• **Fairness + accessibility** → pathway to mass adoption

Check The MVP

A browser-based MVP has been developed to demonstrate the Proof of Witness (PoWit) and Witness Chain (WC) concepts in action. This MVP serves as a functional simulation for concept validation and community feedback.

Check it out here: https://grahambell.io/mvp/

Security note: The MVP runs fully in-browser and does not require wallet connections or personal data.

📝**Note for testers:**
The browser MVP is a concept validation tool proving the core PoWit and WC mechanism. The next phase is developing the first testable P2P version and test it amongst early adopters. So, joining the waitlist enables participants to be a part of the first peer-to-peer test round.

Join Waitlist: https://grahambell.io/mvp/#waitlist

GrahamBell Whitepaper v0.1 (Introductory Edition)

Note: *Detailed technical papers explaining the internal mechanisms of Proof of Witness (PoWit), Proof of Call (PoCall), Witness Chains (WCs), and related systems will be released in upcoming publications.*

Further Reading

https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month

https://www.coinbase.com/blog/coinbases-perspective-on-the-recent-ethereum-classic-etc-double-spend

https://unu.edu/press-release/un-study-reveals-hidden-environmental-impacts-bitcoin-carbon-not-only-harmful-product

https://www.aa.com.tr/en/energy/finance/bitcoin-consumption-beats-argentinas-annual-energy-use/31867

https://www.coindesk.com/tech/2021/05/07/marathon-miners-have-started-censoring-bitcoin-transactions-heres-what-that-means

https://bitcoinmagazine.com/technical/are-mining-pools-becoming-a-problem-

https://github.com/stratum-mining/sv2-spec/blob/main/03-Protocol-Overview.md

https://stratumprotocol.org/docs/

https://hashrateindex.com/hashrate/pools

https://reports.valuates.com/market-reports/QYRE-Auto-31H8470/global-asic-bitcoin-mining-hardware#:~:text=Bee%20Computing-,ASIC%20Bitcoin%20Mining%20Hardware%20Market%20Size,9.3%25%20during%20the%20forecast%20period.