September 20, 2018

Scalable Digital Sovereignty

Technical Brief

www.elixxir.io

Version: 0.7

EXECUTIVE SUMMARY

For blockchain technology and digital currencies to achieve mainstream adoption, consumers require a scalable, high-performing messaging and payment platform that affirms and preserves a user's right to digital sovereignty, without compromising user experience—blockchain performance and convenience. The Elixxir blockchain has been designed to address performance issues hindering the adoption of current decentralized systems, while maintaining the privacy consumers require.

Elixxir provides users with:

- **Speed**: Payment completion and message transmission are completed in a matter of seconds.
- **Transactional privacy**: Only senders and receivers can review and prove payment history. Transaction data is not stored on the blockchain.
- **Communication privacy**: The identity of communicating parties and their devices remains private.

The architecture of the Elixxir platform provides users with performance that scales linearly as computers join the network. Network nodes are incentivized to maximize throughput while ensuring security, and payments use a faster hash-based ownership mechanism instead of digital signatures.

The Elixxir consensus requires nodes work in teams that are sequentially assigned the task of generating blocks as opposed to requiring all nodes to compete individually. Within teams, all nodes are required to independently create cryptographically verifiable proofs that are published alongside the new block, proving that transactions were received and processed properly. Elixxir users are able to validate the integrity of transaction processing using these proofs. Additionally, the existence of just one honest node within the team is sufficient to preserve the anonymity of users.

Elixxir's privacy features are unique and novel capabilities in decentralized technology. Both users and distributed applications enjoy the benefits of a sophisticated anonymization protocol that enables private messaging and transactions. The platform does not store transactions on the blockchain, only tokens, further protecting user privacy.

The team behind the creation of Elixxir is comprised of pioneers of practical, anonymous and verifiable cryptographic systems. Its members are among the first to propose and deploy digital currencies, mix networks, unpermissioned cryptography, anonymous user discovery, verifiable voting systems, and many other advances in cryptography. They have dedicated their collective decades of experience in this space to this breakthrough platform.

Elixxir is capable of replacing current centralized systems at scale and with quick response times. The Elixxir platform targets game-changing verifiability, privacy, and digital sovereignty because, together, they are the digital future.

A LETTER FROM OUR FOUNDER

”Large-scale automated transaction systems are imminent. As the initial choice for their architecture gathers economic and social momentum, it becomes increasingly difficult to reverse. Whichever approach prevails, it will likely have a profound and enduring impact on economic freedom, democracy, and our informational rights.”

”Restrictions on economic freedom may be furthered under the current approach. Markets are often manipulable by parties with special access to information about other participants’ transactions. Information service providers and other major interests, for example, could retain control over various information and media distribution channels while synergistically consolidating their position with sophisticated marketing techniques that rely on gathering far-reaching information about consumers. Computerization has already allowed these and other organizations to grow to unprecedented size and influence; if computerization is continued along current lines, such domination might be further increased. But the computerization of information gathering and dissemination need not lead to centralization: integrating the payment system presented here with communication systems can give individuals and small organizations equal and unrestricted access to information distribution channels. Moreover, when information about the transactions of individuals and organizations is partitioned into separate, unlinkable relationships, the trend toward large-scale gathering of such information, with its potential for manipulation and domination of markets, can be reversed.”

”Attempts to computerize under the current approach threaten democracy as well. They are, as mentioned, likely to engender widespread opposition; the resulting stalemate would yield security mechanisms incapable of providing adequate prior restraint, thus requiring heavy surveillance, based on record-linking, for security. This surveillance might significantly chill individual participation and expression in group and public life. The inadequate security and the accumulation of personally identifiable records, moreover, pose national vulnerabilities. Additionally, the same sophisticated data acquisition and analysis techniques used in marketing are being applied to manipulating public opinion and elections as well. The opportunity exists, however, not only to reverse all these trends, by providing acceptable security without increased surveillance, but also to strengthen democracy. Voting, polling, and surveys, for example, could be conveniently conducted via the new systems; respondents could show relevant credentials pseudonymously, and centralized coordination would not be needed.”

”The new approach provides a practical basis for two new informational human rights that is unobtainable under the current approach. One is the right of individuals to parity with organizations in transaction system use. This is established in practice by individuals’ parity in protecting themselves against abuses, resolving disputes, conferring proxy, and offering services. The other is the right of individuals to disclose only the minimum information necessary: in accessing information sources and distribution channels, in transactions with organizations, and–more fundamentally–in all the interactions that comprise an individual’s informational life.”

”Advances in information technology have always been accompanied by major changes in society: the transition from tribal to larger hierarchical forms, for example, was accompanied by written language, and printing technology helped to foster the emergence of large-scale democracies. Coupling computers with telecommunications creates what has been called the ultimate medium–it is certainly a big step up from paper. One might then ask: To what forms of society could this new technology lead? The two approaches appear to hold quite different answers.”

- David Chaum
1987 [1]

Contents

1 INTRODUCTION

Elixxir is a decentralized blockchain platform that allows users to communicate and exchange value securely and confidentially. Elixxir's breakthrough design produces a decentralized network capable of potentially scaling to process transactions on a mega-tps scale, far exceeding the kilo-tps scale characteristic of conventional mainstream payment systems. The Elixxir design provides users with a blockchain platform that achieves the kind of performance that consumers expect from current centralized systems:

1. **Speed**: Payment processing on the order of seconds, from start to irrevocable finality.
2. **Scale**: Tens of thousands of transactions per second.
3. **True Privacy**: Transactions that are not linked to users or to other transactions. Communications are end-to-end encrypted, they can only be read by the intended recipients.

Elixxir has been designed to realize the vision of a world in which digital sovereignty truly exists, a world in which users can protect themselves and control their privacy by revealing only the absolute minimum amount of information necessary to conduct transactions. Elixxir has been built for the user. Users generate and control their own keys. Users control access to all of their confidential interactions. Users have exclusive access to all their digital property. Users control linkage of any personal credentials to their data. Users are in control of their digital future.

Mainstream adoption of blockchain technology requires a platform capable of scaling to process the necessary high transaction volumes while protecting user's digital sovereignty. To that end, the Elixxir team—led by Dr. David Chaum—has leveraged their experience as innovators in blockchain technology, consensus mechanisms, unpermissioned cryptography, cryptocurrencies, and online voting to address this challenge through the creation of Elixxir.

2 ARCHITECTURE OVERVIEW

In order to protect a user's digital sovereignty, the Elixxir protocol utilizes accelerated mix networks to ensure confidentiality. A mix network [2] is a routing protocol that uses cryptography to dissociate the origin, contents and destination of a message. A message in this context could simply be a text message, or a payment transaction on a blockchain. The Elixxir protocol uses mix networks in combination with a distributed ledger to create a confidential blockchain.

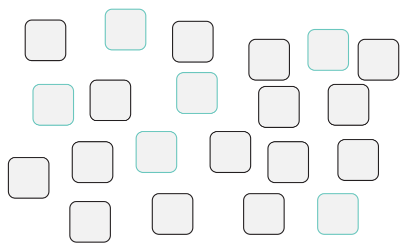


Figure 1: A single team (in teal), randomly selected from a group of nodes

Unlike other blockchain protocols, in the Elixxir protocol, groups of nodes are deterministically organized into teams. Elixxir teams are temporary, and exist only for the duration of the block they are responsible for generating. The team uses a consensus protocol, explained in Section 3, to validate and authenticate operations that anonymize each encrypted message, independently agree to process all messages before decryption, and then independently decrypt [1] and process each message. Following block generation, the team disbands and member nodes become available to be placed on a new random team. As shown in Figure 2, the team allows messages to be sent both directions with anonymity.

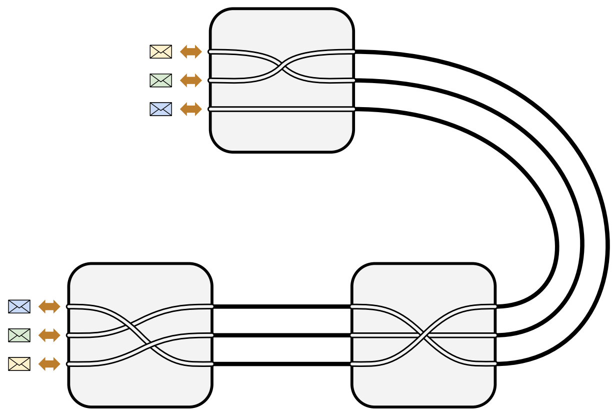


Figure 2: Each team creates an anonymous, verifiable, bi-directional transaction channel to process each block in the blockchain.

All operations conducted by Elixxir teams are accelerated through the use of precomputation [3]. These precomputations produce a template that dictates how the nodes within a team must process information during block generation. Consequently, the template is completely defined before any message information arrives for block generation. The use of precomputation ensures confidentiality while dramatically increasing the speed at which information can be processed to generate a block.

Nodes must be elected to participate in processing the messages and transactions on the Elixxir network. In order to be eligible for election, a node is required to stake tokens on the network. Once elected, a node is eligible to be placed into an Elixxir team.

[1]Messages are still end-to-end encrypted over the network.

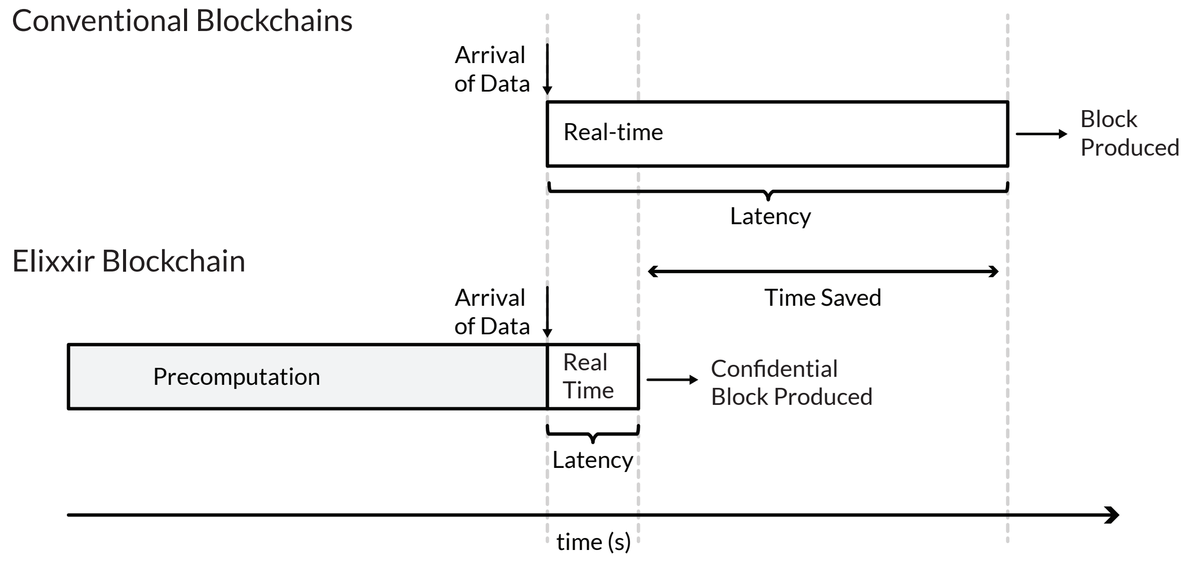


Figure 3: Time-consuming, computationally-intensive team precomputation is performed before transactions are sent or received. This allows very fast real-time computation of transactions to generate each block in the blockchain. The use of precomputation decouples security from latency as seen in conventional blockchains, delivering a greater level of security without the latency penalty.

There are two phases involved in block production by an Elixxir team as depicted in Figure 3. First, the team performs a computationally-intensive precomputation as discussed above, producing a unique template defining how the information or messages of the block will be processed. When messages arrive, the nodes of the team work together to process the messages in real time according to this unique template, a process that takes less than 1/20th of the precomputation time.

Unlike sharding proposals or the lightning network [4], Elixxir teams cannot influence the consensus mechanism's integrity as all aspects of block production are independently predetermined in a strict, verifiable, and immutable manner. Additionally, all nodes in a team independently provide proofs that validate the block prior to final block confirmation.

To ensure proper system functionality, nodes collectively and independently generate cryptographic proofs as commits of batch integrity prior to decryption. In the event that commits do not match, all proofs produced by the nodes can be inspected to identify node failure or malfeasance. Once a malicious or malfunctioning node has been identified, honest nodes refuse further contact and broadcast proof of malfeasance or malfunction to the rest of the network. If a node is verified to be malicious, it loses its stake of tokens, which are burned, and the node is ejected from the network. These, and additional security mechanisms, allow users to prove incorrect handling of their transaction, while rendering them unable to accuse the nodes or the team falsely.

2.1 SCALING STRATEGY

At any given time, tens to hundreds of teams will exist within the network in varying stages of precomputation. However, at any given time, only one team will be producing a block. These precomputations overlap in a cascade, as shown in Figure 4. Consequently, the throughput of the network increases with the addition of more nodes to the network forming more teams. This allows the platform to linearly scale its capacity with the addition of more nodes.

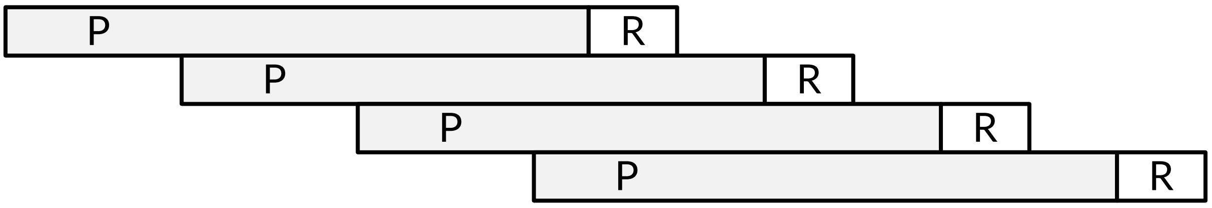


Figure 4: Teams are organized into a cascade pipeline to maximize the number of transactions that can be processed by our platform.

Increasing the number of teams results in increased network resilience as more teams must be brought down to impair or completely disrupt the network. As longer precomputation times become feasible, the number of messages processed by each team can also be increased.

2.2 BLOCK PROPAGATION

Once generated, block data is broadcast to each node in the next team. Once the next active team has received the block data, data is then broadcast to the rest of the nodes in the network. This sequence prioritizes communication to the next team responsible for block generation, ensuring efficient block propagation.

3 CONSENSUS PROTOCOL

The Elixxir consensus protocol is designed to facilitate a blockchain messaging and payment solution that is anonymous and capable of scaling. The Elixxir consensus protocol enables the creation of a resilient, trustless platform that is capable of meeting the diverse array of applications envisioned for the blockchain.

Each node in the team performs the following operations in the Elixxir consensus protocol:

1. Before any transactions are known, the team defines a template comprising commits to message slots for transactions. The template determines, but does not reveal, the order in which each transaction will be processed within the block, and how the transactions will be opened by nodes in the team.
2. Independently, the nodes within the team agree and commit to the transactions without knowing the content of the transactions, and broadcast that commitment to all other team nodes.
3. As a team, the nodes open all transactions together in the predetermined order, revealing their contents. When the team agrees that all transactions are valid, and commits have been made to processing the transactions properly, nodes again broadcast these commits to all other nodes.
4. The team then executes all transactions. Each node independently generates and broadcasts a block that must be identical to the block produced by all other nodes in the team.

The Elixxir consensus has the advantage over other consensus mechanisms in that each node participating in the team provides a short proof that it processed the transactions properly, and publishes that proof as part of the block. Additionally, each team commits to each stage of the block's production before the contents of the block are known. As a result, the output block is a product of the validated input. Any disagreement results in an incorrect proof being attributed to the misbehaving node, which disables that node identity in the network.

3.1 CONSENSUS PROPERTIES

Unlike other platforms, consensus in Elixxir is not vulnerable to a 51% attack, as illustrated in Figure 5. Any single honest node protects team consensus. An entirely dishonest team can only produce proofs for the transactions submitted by the set of users in that round. As such, nodes cannot create fake transactions to their own benefit, nor valid proofs for forged transactions. A completely dishonest team—an unlikely event—is limited to only being able to change the order of transactions, de-anonymizing the transactions, or failing to provide a proof, i.e., faking a failure.

Consensus algorithms in the blockchain space have been primarily hampered by bandwidth limitations; blocks must be propagated to a majority of the system before finality is realized. Even a small block requires exponentially more bandwidth than its file-size

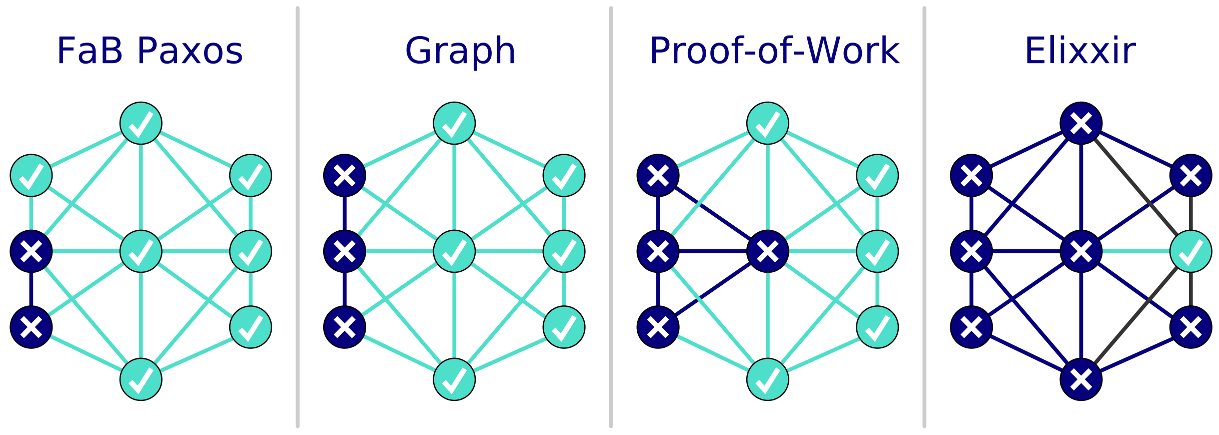


Figure 5: The number of honest (green) nodes, hashrate units, or stakes required to achieve consensus in a 9-unit configuration. Unlike graph and traditional proof-of-work (and -stake) solutions, Elixxir consensus requires only a single honest node to perform user-verifiable operations.

to transfer across a network. In the Elixxir consensus protocol, nodes reach finality by evaluating short proofs that are propagated optimally through the network. As a result, the Elixxir consensus mechanism facilitates seconds-long finality times.

3.2 TEAM RESILIENCE

The Elixxir protocol has a built in timeout period. A team's failure to complete a block by the timeout period requires clients to resubmit their transactions to another team for processing. For this delay, the failing team does not receive any token revenue for computational work. Team nodes may face further repercussions, such as failing to be re-elected to the network, as failure metrics are publicly available. The potential penalties incentivize nodes to provide resilient network connectivity to ensure that teams they participate in complete block generation. Attackers are dissuaded as well because the teams are constantly moving, unpredictable targets, forcing asymmetric attack patterns to affect network stability.

As network team size increases, the probability of a node impacting completion of a block increases, so the primary engineering trade-off for resilient block generation is the size of the teams. Also, as team sizes grow, the real-time processing times increase and throughput decreases. Team sizes should range from 5 to 30 nodes to produce a system that exhibits seconds-long block generation. Such team sizes compare favorably with the entirety of the controlling interest[2] in other networks.

3.3 NETWORK RESILIENCE

The Elixxir platform has been designed to incentivize nodes to follow the rules of the protocol. Failure to do so results in penalties for all nodes in teams containing malicious

[2]For example, 21 nodes control the EOS network, and 5 mining pools control Bitcoin. (`https://www.ccn.com/bitmains-mining-pools-now-control-nearly-51-percent-of-the-bitcoin-hashrate/`)

or unproductive nodes. Nodes are incentivized to allow the protocol to operate without interference. The protocol also offers significant flexibility when dealing with network failures. The set of valid nodes is known, as they must have been elected to join the network. Since the teams are arranged in a cascade, the failure of any one team can be readily mitigated by the next team in the cascade.

Successfully interrupting block generation would require all scheduled teams to be disabled. The most common failures—individual node failures, geographical outages, an entire country being taken offline, etc.—are handled without affecting platform operation. When a targeted, extended, large-scale network attack does successfully disable all scheduled teams, the platform is capable of supporting the same recovery mechanisms found in other systems, like “longest chain/most computation wins”.

3.4 PARTICIPATORY EQUALITY

The egalitarian properties achieved by Elixxir compare exceptionally favorably to other consensus mechanisms. Specifically, the greater computational capability or larger stake of a node does not advantage that node over others in this platform.

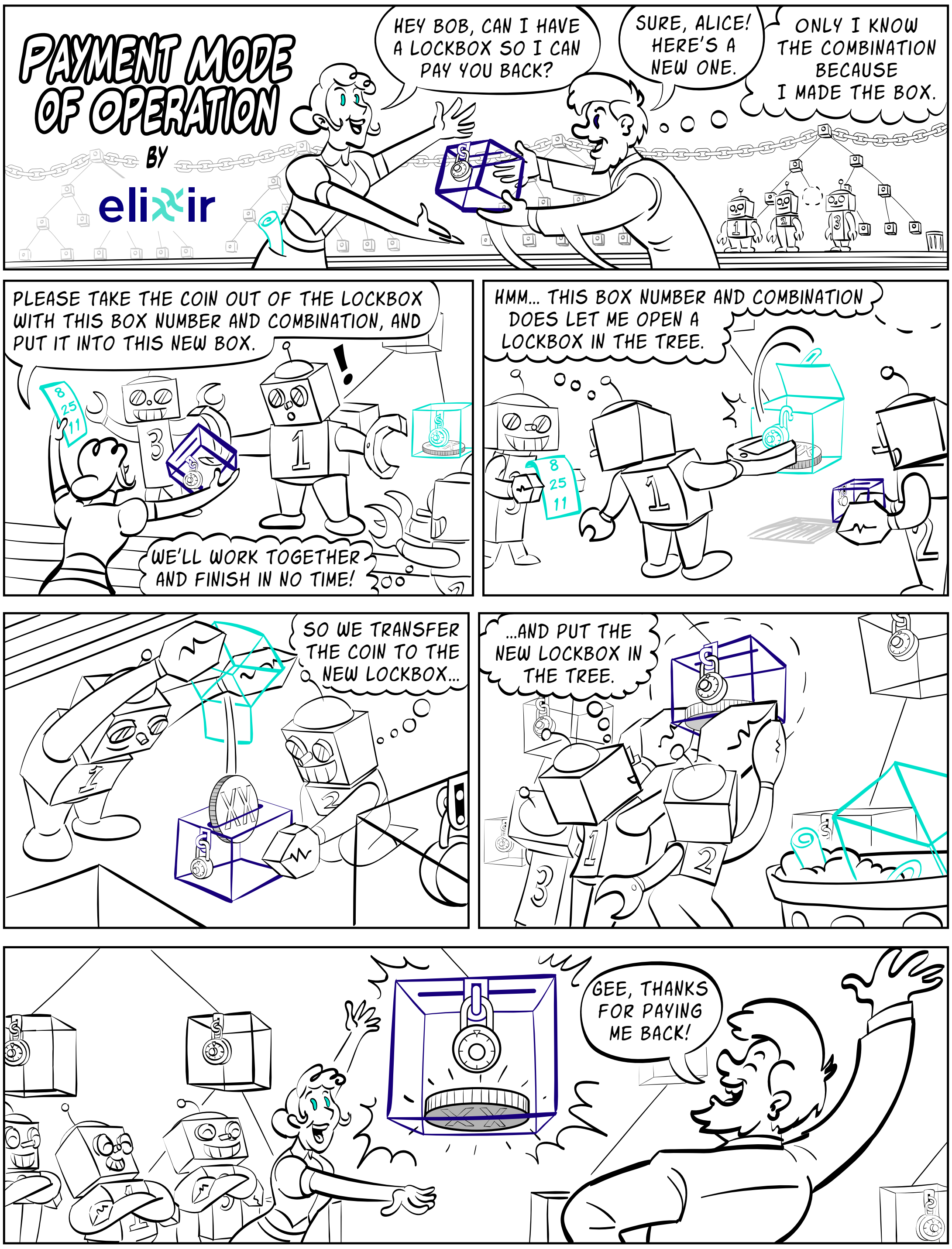
The successful completion of a block is a cryptographically secured group computation analogous to a proof of useful work. One can think of processing the transactions as a mining operation where the work is not wasted, but directly corresponds to providing the properties of the platform. Hence, any unforeseen algorithmic advances, new ASIC designs, or other developments do not advantage one team or node over another. Additionally, each node is treated equally and each one automatically audits the fidelity of all other nodes.

3.5 SYBIL ATTACK RESISTANCE

Within the Elixxir protocol, sybil attack [5] resistance is created through the use of verifiable real-time inter-node performance testing, staking, and elections. *Staking* requires nodes to place a governance-determined number of tokens in an “escrow” that will be burned if they are expelled from the system for malfeasance.

Elections in Elixxir utilize methodologies such as random sample voting [6] and decoy balloting for honest and trustworthy elections by which users of the system can elect which nodes are verified to join teams, and which can be excluded. All elections in the Elixxir platform will use cryptographically secured, voter-verifiable, end-to-end election protocols. The Elixxir team has pioneered these protocols, being the first to propose such systems [7], the first to deploy them in a binding governmental election [8], and the first to use a blockchain for publishing election data in an election [9].

4 PAYMENTS


PAYMENT MODE OF OPERATION
BY
elixxir
HEY BOB, CAN I HAVE A LOCKBOX SO I CAN PAY YOU BACK?
SURE, ALICE! HERE'S A NEW ONE.
ONLY I KNOW THE COMBINATION BECAUSE I MADE THE BOX.
PLEASE TAKE THE COIN OUT OF THE LOCKBOX WITH THIS BOX NUMBER AND COMBINATION, AND PUT IT INTO THIS NEW BOX.
8 25 11
!
WE'LL WORK TOGETHER AND FINISH IN NO TIME!
HMM... THIS BOX NUMBER AND COMBINATION DOES LET ME OPEN A LOCKBOX IN THE TREE.
SO WE TRANSFER THE COIN TO THE NEW LOCKBOX...
...AND PUT THE NEW LOCKBOX IN THE TREE.
GEE, THANKS FOR PAYING ME BACK!

Token handling in the Elixxir platform has some unique attributes. Token handling in most conventional blockchain systems today is wallet-based. In the Elixxir protocol, token handling is token based, meaning the token remains static, while a secret is required to prove ownership. These secrets are kept off-chain and change when ownership of a token is assigned to a new owner.

Elixxir secures individual tokens rather than securing an entire wallet as a whole. Each token owned by a user is secured through knowledge of an individual secret, which means that even if an attacker successfully performs a brute-force attack, only one single token from the user can be compromised.

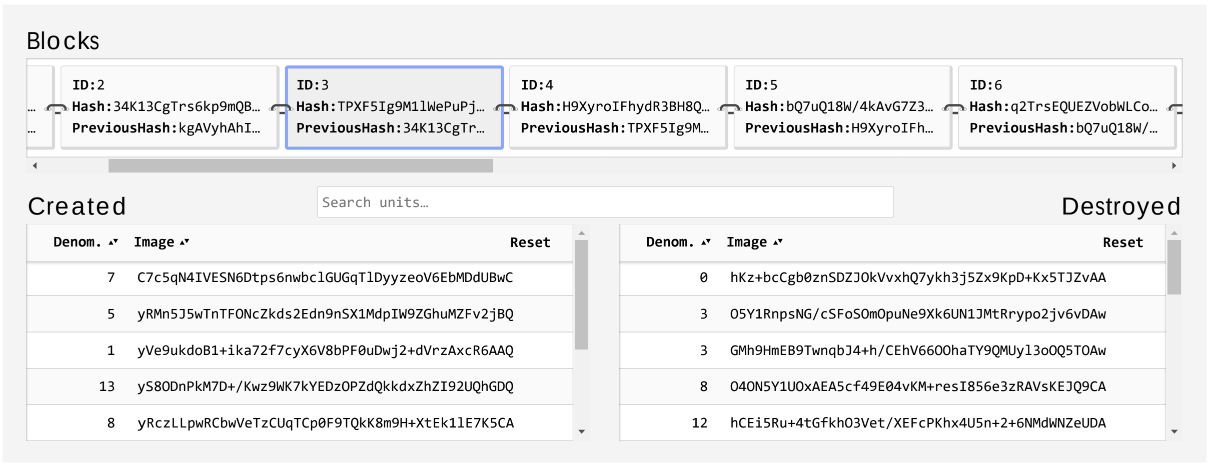
Elixxir blocks do not contain any information about transactions, i.e. sender, receiver, and amount. Instead, a block from the Elixxir blockchain contains assignments of tokens to addresses belonging to the payee, and previous addresses belonging to the payer. Moreover, there is no information linking payer and payee in the blockchain, which translates into on-chain unlinkability.

4.1 BLOCK STRUCTURE

Elixxir takes a new approach to the information contained in blocks. Each block contains nothing more than unordered lists of the past and new addresses to which tokens were assigned by the transactions of that block.

By analyzing the entire blockchain, an observer is unable to link the transacting parties or the features of the transaction to one another (i.e., how many were sent). As a result, one can only infer that in a specific block a set of tokens have been unlinkably assigned to new addresses from old addresses.

To contextualize such block information, we show a snippet of what is present in the Elixxir block explorer tool in Figure 6.


Blocks

ID:2	**ID:**3	**ID:**4	**ID:**5	**ID:**6
Hash:34K13CgTrs6kp9mQB…	**Hash:**TPXF5Ig9M1lWePuPj…	**Hash:**H9XyroIFhydR3BH8Q…	**Hash:**bQ7uQ18W/4kAvG7Z3…	**Hash:**q2TrsEQUEZVobWLCo…
PreviousHash:kgAVyhAhI…	**PreviousHash:**34K13CgTr…	**PreviousHash:**TPXF5Ig9M…	**PreviousHash:**H9XyroIFh…	**PreviousHash:**bQ7uQ18W/…

Created

Search units…

Denom.	Image	Reset
7	C7c5qN4IVESN6Dtps6nwbclGUGqTlDyyzeoV6EbMDdUBwC	
5	yRMn5J5wTnTFONcZkds2Edn9nSX1MdpIW9ZGhuMZFv2jBQ	
1	yVe9ukdoB1+ika72f7cyX6V8bPF0uDwj2+dVrzAxcR6AAQ	
13	yS8ODnPkM7D+/Kwz9WK7kYEDzOPZdQkkdxZhZI92UQhGDQ	
8	yRczLLpwRCbwVeTzCUqTCp0F9TQkK8m9H+XtEk1lE7K5CA	

Destroyed

Denom.	Image	Reset
0	hKz+bcCgb0znSDZJOkVvxhQ7ykh3j5Zx9KpD+Kx5TJZvAA	
3	O5Y1RnpsNG/cSFoSOmOpuNe9Xk6UN1JMtRrypo2jv6vDAw	
3	GMh9HmEB9TwnqbJ4+h/CEhV66OOhaTY9QMUyl3oOQ5TOAw	
8	O4ON5Y1UOxAEA5cf49E04vKM+resI856e3zRAVsKEJQ9CA	
12	hCEi5Ru+4tGfkhO3Vet/XEFcPKhx4U5n+2+6NMdWNZeUDA	

Figure 6: Block #3 from the Elixxir Block Explorer

Within both the block and the nodes, data is stored as a binary radix tree combined with a Merkle tree [10]. This structure allows for fast searching and rehashing of the root within the nodes, and for proofs to be generated that verify the existence of a token within a block. This is achieved simply by revealing the hashes of the block root, the token, and all non-leaf data blocks in between. As a result, shorthand proofs can be generated and used for validation in lieu of requiring all of the data of a relevant block referencing the transaction of interest.

4.2 PAYMENT PRELIMINARIES

Normally, in the blockchain space, users submit a transaction—signed with their corresponding private key—to the system. The nodes in the system then check the validity of the transaction by employing the user's corresponding public key. If the key is valid and the user has funds to perform the payment, then the transaction is written to a block.

Elixxir introduces a new and faster concept: *Hash-Based Ownership*. Since hash functions are considered infeasible to invert, users can use pre-images as proof of their ownership of specific images. By chaining this process of revealing these pre-images with our Elixxir protocol, users are able to perform payment transactions anonymously and securely. Furthermore, this process ensures that no one is able to forge a fake transaction in an attempt to steal someone's tokens.

4.3 MAKING A PAYMENT

A simplified payment transaction in the system starts with an invoice. Bob sends Alice an invoice containing the destination address (where she should send the money). This address is an image (the output of a hash function) that Bob previously generated from a random preimage (a secret that is the input to a hash function).

Alice, after receiving the destination image (address), submits a payment transaction to the system. This transaction contains the preimage (secret) of a token she owns along with the image (address) from Bob's invoice.

The system checks whether the preimage (secret) Alice sent is valid and exists in the ledger and then transfers the specified amount from Alice's token to Bob's destination image (address). After processing the transaction successfully, the system returns a proof receipt to Alice that she can share with Bob, which validates that the transaction executed correctly.

This receipt provides proof that the transaction is properly recorded in the block by providing the Merkle path within the block of those tokens. This alone is enough proof that the transfer took place correctly and that, therefore, the tokens now belong to Bob. However, both parties (Alice or Bob) can freely check the blockchain and verify that the destination image (address) and the proper amount are present in the corresponding block.

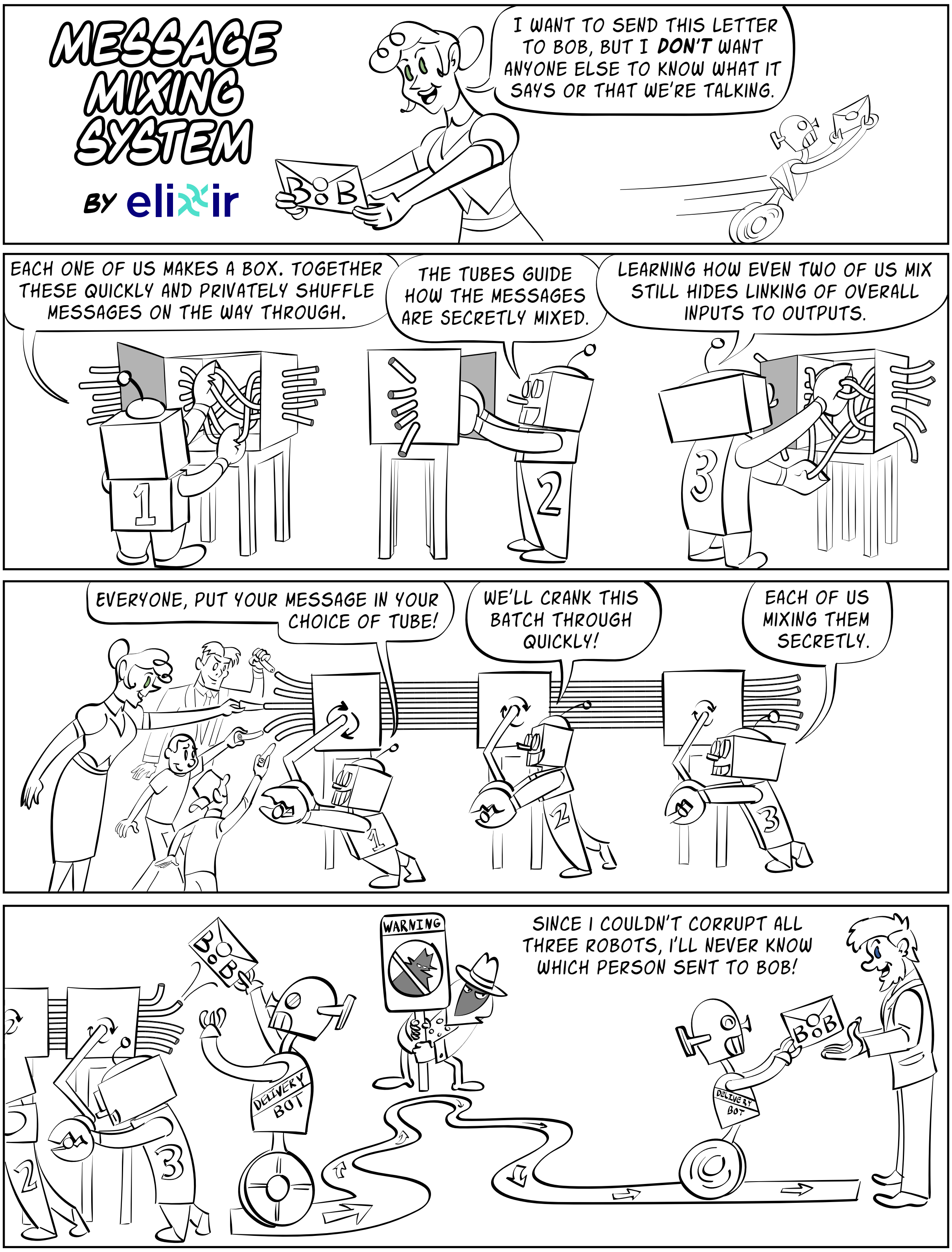
Elixxir's unique architecture and payment processing mechanisms offer three advantages over traditional approaches:

1. User confidentiality is protected by the limited information that is available on-

chain.
2. Security is increased substantially by securing tokens instead of wallets. In the exceptionally rare event that a successful brute-force attack does occur, security of at most one token may be affected.
3. Transaction processing is faster because hash-based ownership can be completed in a fraction of the time required for a digital signature in traditional blockchain platforms.

As others have said [11], when contrasting digital signatures characteristic of traditional blockchain platforms to hash-based digital signatures used in the Elixxir platform, *”Every signature scheme uses a cryptographic hash function; hash-based signatures use nothing else.”* Lastly, unlike digital signatures, hashes are secure against quantum-computational capabilities.

5 MIXING MESSAGES AND TRANSACTIONS


MESSAGE MIXING SYSTEM BY elixxir
BOB
I WANT TO SEND THIS LETTER TO BOB, BUT I DON'T WANT ANYONE ELSE TO KNOW WHAT IT SAYS OR THAT WE'RE TALKING.
EACH ONE OF US MAKES A BOX. TOGETHER THESE QUICKLY AND PRIVATELY SHUFFLE MESSAGES ON THE WAY THROUGH.
THE TUBES GUIDE HOW THE MESSAGES ARE SECRETLY MIXED.
LEARNING HOW EVEN TWO OF US MIX STILL HIDES LINKING OF OVERALL INPUTS TO OUTPUTS.
1
2
3
EVERYONE, PUT YOUR MESSAGE IN YOUR CHOICE OF TUBE!
WE'LL CRANK THIS BATCH THROUGH QUICKLY!
EACH OF US MIXING THEM SECRETLY.
WARNING
DELIVERY BOT
SINCE I COULDN'T CORRUPT ALL THREE ROBOTS, I'LL NEVER KNOW WHICH PERSON SENT TO BOB!

Each team in the Elixxir platform runs a single instance of a mixing network (mixnet) based on the cMix protocol [12]. Mixnets anonymize batches of messages and transactions, while protecting the confidentiality and integrity of each message. Besides supporting secure communications between users, these features are leveraged, and expanded to provide key functionality for the Elixxir consensus protocol.

The cMix protocol is a breakthrough itself: it exhibits drastically lower real-time cryptographic latency than any other mixnet. By using a precomputation, the core cMix protocol eliminates all expensive real-time public-key operations performed on behalf of senders and recipients, and by nodes. This decreases real-time latency and lowers computational costs to clients. The core real-time phase, the second phase in the activity of a team, requires only a few quick computations, making it very well suited to applications running on lightweight clients, including chat messaging systems on smartphones, applications on low-power devices, and—most important—transaction processing.

Message processing in cMix involves 3 operations: Reception, Permutation, and Delivery. During Reception, masking network encryption is added to each already end-to-end encrypted message, while user-to-network encryption is removed from it, disassociating the senders identity from the message. In Permutation, the order of messages within a batch is shuffled, removing an observer's ability to correlate the order in which messages were received with the senders' identities. Finally, during Delivery, each node independently removes all masking network encryption, and sends the end-to-end encrypted message to its labeled destination.

The cMix Protocol has three additional important features that make it unique:

- **Return Path**. The return path allows a receiver to send an immediate response through the mixnet; this permits receipts of transactions to be returned to users without the platform needing to know addressing information, thereby hiding the identity of the sender. To accomplish this goal, nodes generate additional keying material for the return path, and apply an inverse permutation so that responses arrive at the original senders.
- **Commitments**. Commitments are a protocol that produces data, often produced through hashing, that allows a third party to audit a computation performed by a node at a later date [13]. All messages exchanged between nodes, the permutations they perform, and all keying materials in the mixnet's precomputation inherently function as commitments of how messages will be processed in the future, during the real-time phase of block generation. Nodes also produce a commit of the batch of encrypted messages before any decryption takes place. Commits function as an efficient mechanism for verifying that nodes perform their operations correctly.
- **Group Opening**. During the delivery operation, before each node in a team decrypts the batch of messages they have received, they create a commit of the batch, confirm with one another that all commits are identical, and then proceed to de-

crypt the batch independently. This guarantees that all nodes in the team work on the same content before any sensitive information is received. This prevents any single node from accessing sensitive information when other nodes are excluded from having the same access. This ensures that all honest nodes in the team are empowered to protect the integrity of the team and the properties they provide, namely confidentiality and anonymity.

With these features, Elixxir provides integrity and anonymity for users sending messages and transactions through the platform. In Elixxir, any honest node can, with non-negligible probability, identify nodes that violate integrity, and prevent malicious nodes improperly indicting an honest node. Lastly, any single honest node is able to protect user anonymity.

6 CONCLUSION

Elixxir is designed to enable true digital sovereignty for the first time by giving users the privacy and speed they expect. Elixxir team members have built on decades of innovation in cryptographic systems—much of it their own—to create a platform that uniquely ensures the integrity and privacy of digital assets and communications. With Elixxir, no-one can read your messages or steal your money. Period.

The Elixxir platform protects privacy through an anonymous mixnet protocol, and a blockchain that stores tokens, not transactions. Likewise, it achieves finality quickly by abandoning the use of traditional signature-based payment processing in favor of hash-based authentications. This is achieved through the platform's unique consensus mechanism, whereby a group of system nodes works as a team, with integrity guarantees provided via verifiable proofs. In Elixxir, future improvements in computational power translate directly to block finality being realized more quickly, and the architecture enables linear scaling of block processing as the network grows.

Elixxir design is unique in being able to, for the first time, scale to provide users globally with a high performing payment and messaging solution that affirms and preserves their right to digital sovereignty.

7 REFERENCES

[1] David Chaum. "Security Without Identification: Transaction Systems to Make Big Brother Obsolete". In: *Commun. ACM* 28.10 (Oct. 1985), pp. 1030–1044. ISSN: 0001-0782. DOI: 10.1145/4372.4373. URL: https://www.chaum.com/publications/Security_Wthout_Identification.html.

[2] David Chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". In: *Communications of the ACM* 24.2 (Feb. 1981).

[3] Ernest F. Brickell et al. "Fast Exponentiation with Precomputation (Extended Abstract)". In: *Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings*. 1992, pp. 200–207. DOI: 10.1007/3-540-47555-9_18. URL: https://doi.org/10.1007/3-540-47555-9%5C_18.

[4] Joseph Poon and Thaddeus Dryja. *The bitcoin lightning network: Scalable off-chain instant payments*. Tech. rep. Technical Report (draft). https://lightning. network, 2015.

[5] John R. Douceur. "The Sybil Attack". In: *Revised Papers from the First International Workshop on Peer-to-Peer Systems*. IPTPS '01. London, UK, UK: Springer-Verlag, 2002, pp. 251–260. ISBN: 3-540-44179-4. URL: http://dl.acm.org/citation.cfm?id=646334.687813.

[6] David Chaum. *Random Sample Voting*. https://rsvoting.org/whitepaper/white_paper.pdf. Accessed: 2018-09-11.

[7] David Chaum. "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA". In: *Advances in Cryptology — EUROCRYPT '88*. Ed. by D. Barstow et al. Berlin, Heidelberg: Springer Berlin Heidelberg, 1988, pp. 177–182. ISBN: 978-3-540-45961-3.

[8] Richard Carback et al. "Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy". In: *19th USENIX Security Symposium*. USENIX Association. Washington, DC, USA, Sept. 2010. URL: http://carback.us/rick/papers/carback-tpcasestudy-2010-usenix.pdf.

[9] Jeremy Clark and Aleksander Essex. "CommitCoin: Carbon Dating Commitments with Bitcoin". In: *Financial Cryptography and Data Security*. Ed. by Angelos D. Keromytis. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 390–398. ISBN: 978-3-642-32946-3.

[10] Ralph Charles Merkle. "Secrecy, Authentication, and Public Key Systems." AAI8001972. PhD thesis. Stanford, CA, USA, 1979.

[11] Daniel J. Bernstein et al. "SPHINCS: Practical Stateless Hash-Based Signatures". In: *Advances in Cryptology – EUROCRYPT 2015*. Ed. by Elisabeth Oswald and Marc Fischlin. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 368–397. ISBN: 978-3-662-46800-5.

[12] David Chaum et al. “cMix: Mixing with Minimal Real-Time Asymmetric Cryptographic Operations.” In: *ACNS*. Ed. by Dieter Gollmann, Atsuko Miyaji, and Hiroaki Kikuchi. Vol. 10355. Lecture Notes in Computer Science. Springer, 2017, pp. 557–578. ISBN: 978-3-319-61204-1. URL: `http://dblp.uni-trier.de/db/conf/acns/acns2017.html#ChaumDJKKRS17`.

[13] Shai Halevi and Silvio Micali. “Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing”. In: *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*. CRYPTO ’96. London, UK, UK: Springer-Verlag, 1996, pp. 201–215. ISBN: 3-540-61512-1. URL: `http://dl.acm.org/citation.cfm?id=646761.706019`.