Technical Questions and Answers

Question: ***What does Gorbyte have, in order to substitute Bitcoin's "proof of work"?***

In PoW networks, miners provide two types of security functions: a) transaction security, through encryption and verification, and b) security against majority attacks against the network.

Gorbyte maintains the first type of security in all of its nodes. However, the responsibility for security against DoS and majority attacks is decentralized. For example, suppliers of BRUD devices are publicly accredited, and are asked to provide uniquely identifiable devices (more in point 2, below).

1. In Gorbyte, attempts to influence its consensus mechanism are fruitless and provide no practical advantage to the attacker.
The Gorbyte design provides no rewards for being the first to complete a Block (No mining rewards) and no rewards for assembling transactions (no transaction fees). Gorbyte users share their processing resources by running a full node, and get value by being able to use Gorbyte's services.
These are: free basic transactions, stable currency, no fee savings account, profit sharing, secure messaging, person-to-IoT communication, and many other distributed application services currently being developed.
Since the Gorbyte design does not include a way to create new currency, another opportunity for attack is removed.
In any case, such attacks would influence the resulting block only if the attacker controlled the majority of nodes.

2. Majority attacks are handled by our BRUD device architecture.
Each Gorbyte node needs to establish a few random sessions (a logical neighborhood) with physically dispersed peers. At session establishment, the node address is associated to a virtual, or real, blockchain-registered unique device (BRUD). Thus our nodes are unique. Potential attackers are prevented from simulating and proliferating virtual network nodes and mount majority attacks. No proof of work is needed. Node transaction requests can now be limited (e.g.: to about one per minute) to prevent DoS attacks.

Specific types of attack are described in “The BRUD Architecture”, Appendix E at: http://gorbyte.com/documents/The%20BRUD%20Architecture.pdf

Question: ***Why is Gorbyte scalable?***

Scalability can be a problem when some resource requirements grow exponentially with the number of nodes in the network. For example, the time to distribute or process transactions, or the time to process a block, or the communication time to distribute a block, or the space required for storing a block, or the space/time required to store and process unconfirmed transaction, etc.

In a system, these parameters can be kept in check, to a point, with an efficient design. However, any system will have limits, given the technology at that time.

The researchers at Gorbyte, Inc. provide two answers to scalability.

1. More than a one hundred fold improvement in throughput, (See transactions per second calculation in the answer to the next question), and
2. Off-loading the blockchain by supporting general distributed applications (GApps). These are applications that can use the blockchain, but run off the blockchain.

1. Improvement in throughput: Current PoW crypto-networks are not designed for efficiency and most of the above example parameters will tend to grow faster than the number of miners in the network. One of the reasons is that the PoW system is not truly decentralized, but randomly centralized. Another reason is that most of the miners' processing power is used for a conceptually simple task: to select a random "real" miner. PoS systems should do better, but are as yet unproven.

Gorbyte uses a more decentralized design for its consensus process:

- Every node participates in the consensus agreement process.
- Every node communicates only with a small number of random logical neighbors.
- The reconciliation communication among all nodes happens in parallel.
- Several precautions are taken in order for blocks to be similarly assembled by every node, at the start of reconciliation (e.g.: synchronous operation, canonical ordering of transactions, no picking and choosing of transactions by miners).
- Only in a small percentage of cases a node will require information from outside its logical neighborhood.

Thus the agreement process requires a small amount of time and much less processing power.

If a node cannot reach an agreement within a predefined time (e.g.: delay or malfunction), it will have to reinitialize and get the last block from an active peer node.

For the above reasons, Gorbyte is **not bound by processing power**, but by communication broadcast and download times.

Considering also the exponential improvements in new technologies, we predict that the Gorbyte architecture will remain scalable. That is, the increased demand for new resources (e.g. bandwidth, memory, processing power) is expected to continue to be satisfied as the number of nodes in the network grows.

2. Off-loading the blockchain: The second answer to the problem of scalability is provided by Gorbyte's BRUD device architecture.

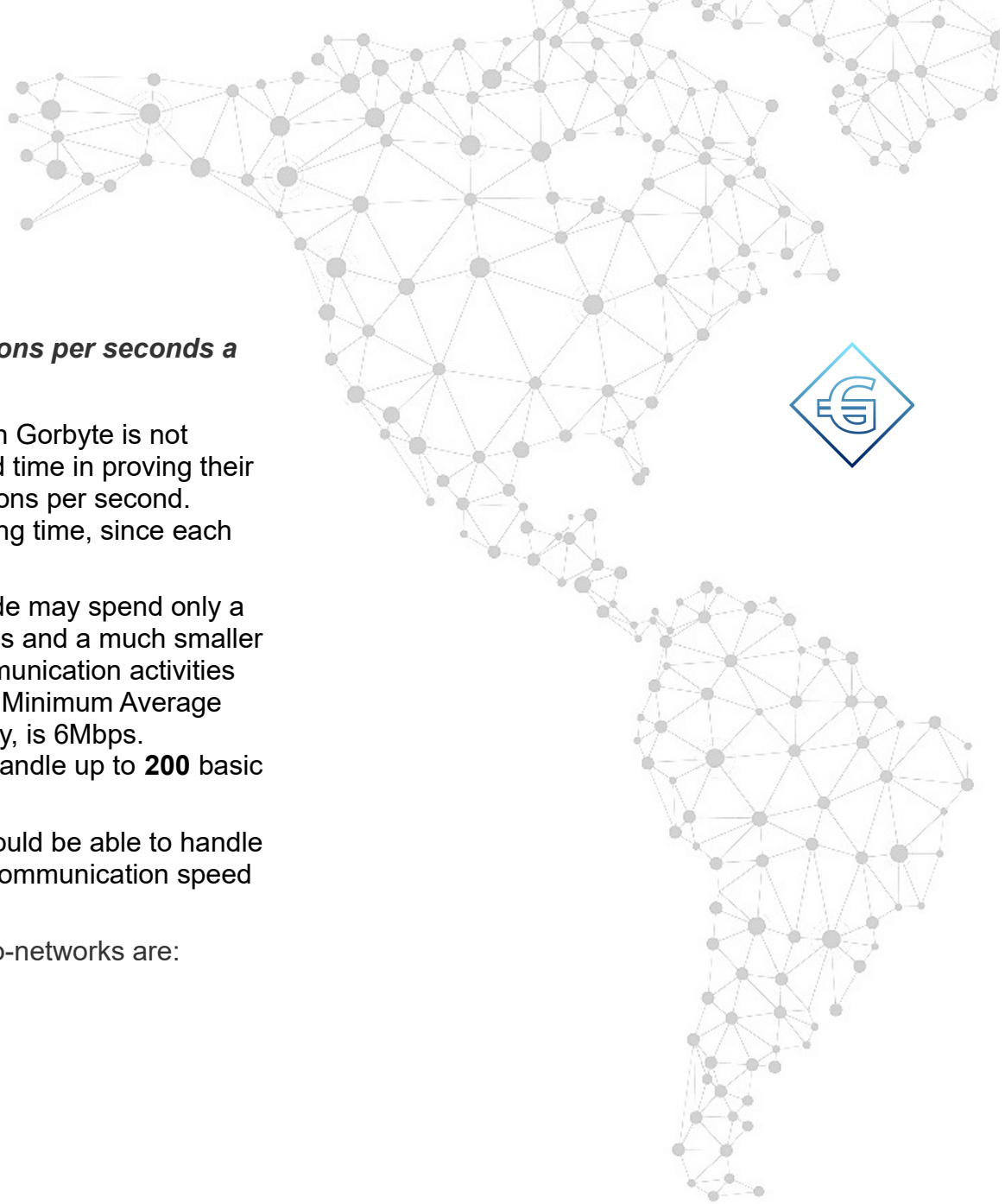
Gorbyte, in addition to supporting smart contracts (DApps), will support general distributed applications (GApps) that are able to use the blockchain for critical events and historical data, but run off the blockchain. For most applications, this greatly reduces the amount of processing and storage requirements on the blockchain, thus allowing the blockchain to be usable by the much larger market of general distributed applications without the limitations imposed by smart contracts.

Smart contracts are objects stored on the blockchain, running on the blockchain and producing results on the blockchain. Thus any input, execution or output event on such objects involves the blockchain and, by definition, it is replicated on all the network nodes.

While there is a need for smart contracts for critical applications, the majority of general distributed applications (an estimated five sixths of the total software market) will need to store only critical events and information on the blockchain, but can do most of their processing and data manipulation using resources off the blockchain.

The availability of GApps will reduce the requirement to develop every blockchain application using the only tool currently available (smart contracts), thus at the same time it will:

- greatly reduce the throughput and storage requirements of the crypto-network, and
- allow for an expansion of the type and range of general distributed applications taking advantage of the blockchain.



Question: ***What is the maximum number of transactions per seconds a Gorbyte node can handle?***

The maximum number of transactions per second (tps) in Gorbyte is not bounded by processing power, since nodes do not spend time in proving their processing power and are capable of millions of instructions per second. They are instead bounded by communication broadcasting time, since each transaction has to be received by every node.

In the most conservative scenario, we assume that a node may spend only a sixth of its time receiving transaction broadcast messages and a much smaller smaller amount of time on other blockchain-related communication activities (outside of reconciliation time). We also assume that the Minimum Average Download Speed, for Gorbyte participating devices, today, is 6Mbps. Under these assumptions, a Gorbyte node today could handle up to **200** basic transactions per second (500 bytes average length).

In a realistic scenario, three years from now, Gorbyte should be able to handle up to **6400** tps. This number will grow with the average communication speed available to users for their devices.

The number of transactions per second for current crypto-networks are: Bitcoin, **3-7** tps; Ethereum **7-15** tps.