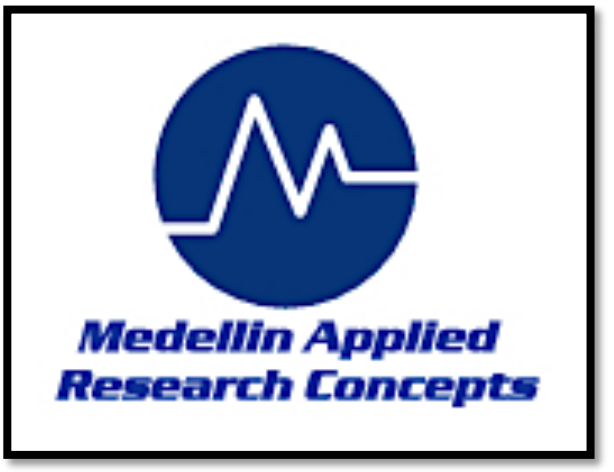


GATED ARRAY BLOCKCHAIN ENABLED DEVICES

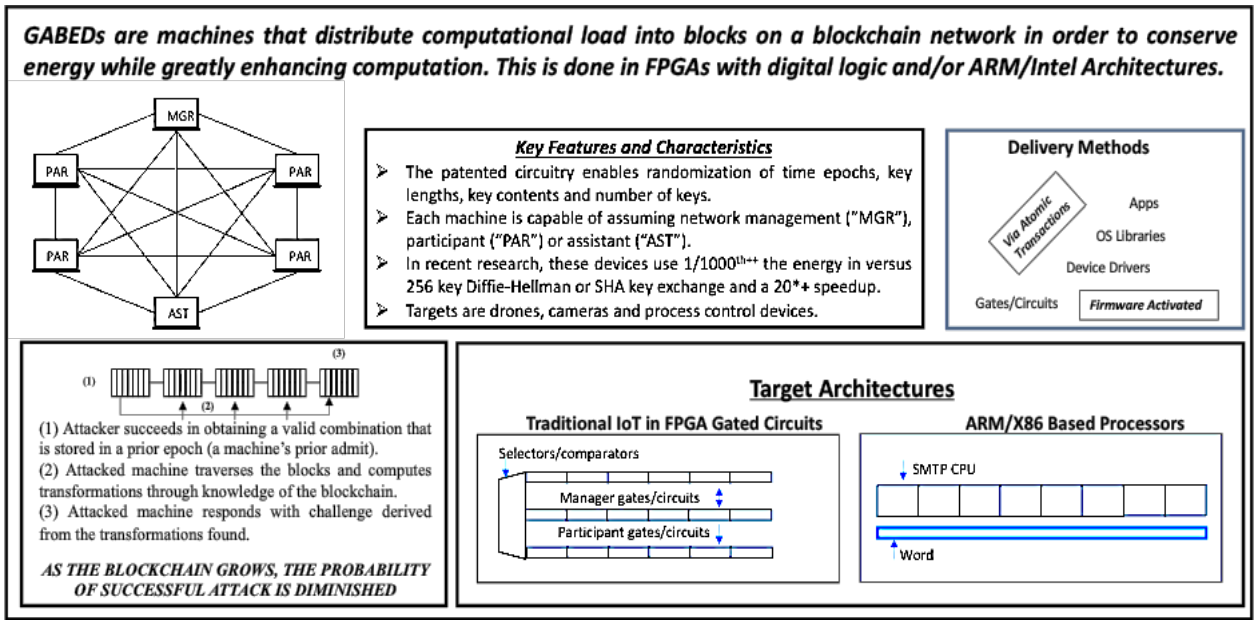
Concept Description White Paper –
Uncrewed Autonomous System Version

March 2026

Medellin Applied Research Concepts, LLC
Highland Village, Texas
www.mede-arc.com

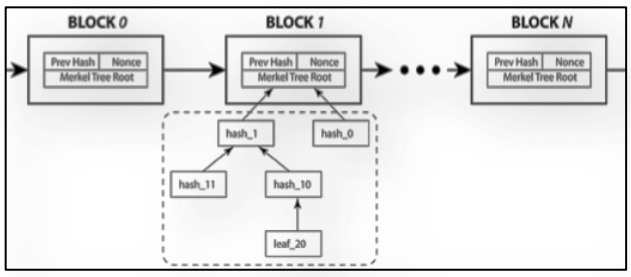
Introduction

GABEDs are a technological innovation that will dramatically increase the security over existing methods [AES-256] with a fraction of the compute time [1/20th] and energy needed [1/1,000th or less]. GABEDs implement blockchain patterns in gated arrays and other types of digital and analog architectures. Key features include the ability to randomize the consensus process (when valid blocks get appended), the contents of the blocks in the chain and regeneration of keys at random time intervals (aka "epochs"). "Shared intelligence" is achieved when machines have complete knowledge of the blockchain (duration, encryption, encryption changes, admitted blocks and encryption patterns) and can establish logically verified properties of identity, trust, contract and value transfer in a cumulative randomized cryptographic environment. The resulting attack surface is confused by these time-dimensioned changes creating chaos for the un-informed hacker thus significantly hindering harmful outcomes. GABEDs today implement ultra-secure command transfers and provide secure evidence of mission completion on SRS, Inc. UAS products and are ready for extension to other UAS products.



A Blockchain records information in a way that is very difficult to change or decipher. The technology achieves this by grouping and storing identical copies (blocks) of information across a network of computers instead of a central location. The blocks are linked together in a chronological "chain." New information is bundled in a block and verified by multiple computers across the network through a consensus process. The block is cryptographically linked to the previous block by the verifying entity, creating a tamper-resilient permanent chain. Intrusion requires knowledge of the current block but also preceding blocks and other anomalies of the chained blocks.

A Typical Blockchain



Randomization of Attack Surfaces

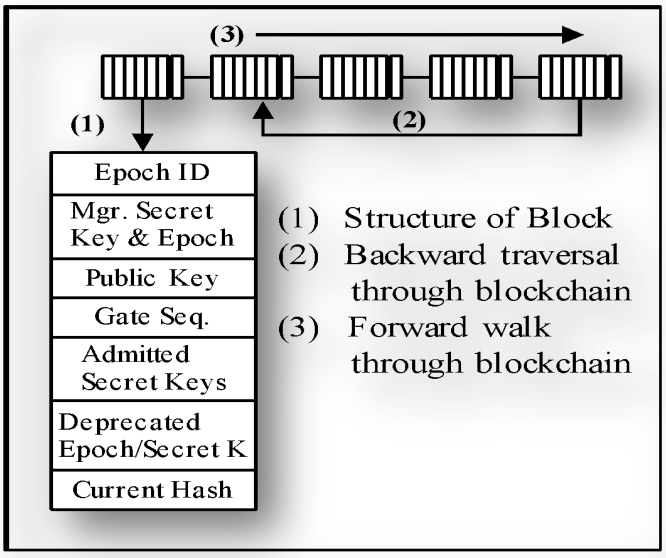
GABEDs use randomized, embedded blockchain encryption and a novel communication protocol that does not rely on permissioned networks but allows nodes to organically establish identity and trust. Ground Control Systems (GCS) can operate as a "blockchain network manager" (generating blockchain keys and epochs) or as a "participant," communicating by storing relevant "keys" using blocks in their blockchain memories. The blocks interact via key exchanges and certain identity blocks "regenerate" randomly over time slices called "epochs". An "epoch" duration is determined randomly and it serves to regenerate key components of the network of blockchain nodes with new unique random blocks. The machines are able to validate blockchain membership through logical operations using certain blocks exchanged in a dialogue.

The use of epochs is a revolutionary component of the GABEDs' protocol and introduces randomness into the system that enhances security and resilience by making key regeneration and block additions extremely difficult to predict and therefore significantly degrading cyber-attack success. As the dialogues progress, trust is established and the nodes ultimately enter into value exchanges that are recorded in the blockchain and shared for intelligence across the blockchain participants. The record of successful transfer is published as an additional block to the blockchain network and the images are redundantly stored by the UAS and its GCS paired unit (the entity that has negotiated keys and requested the operation).

The resulting randomization of key parameters frustrates hackers, confuses and significantly minimizes the attack surface for aggressors. As time progresses, these randomized parameters have a compounding effect, making it exceedingly difficult for malicious intruders to establish a network foothold and sustain it (see "Blockchain Structure & Traversal Example"). In peer-reviewed publications (reference 2) GABED demonstrates high survivability when tested against five common cyber-attack vectors including brute force, denial of service, credential simulation, impostor, and machine control (hijacking with insider knowledge).

The randomization of parameters within the GABED is critical to understanding how this technology changes the game. These include the duration of time between regeneration of keys (epochs), the lengths of keys (binary digits), number of keys, direct election of network managers and assistant managers - which themselves can be shuffled from epoch to epoch. Applied together, the parameter randomization results in a 1 in 2^36 (0.000000015% chance) probability of successful attack (reference 2).

Structure & Traversal Example (Ref. 1)



Formal Logic and Computational Distribution

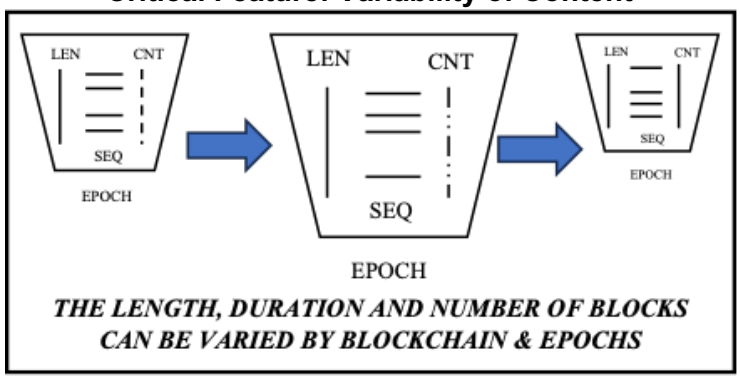
Two fundamental principles make the GABED enable efficiency in key negotiation and encryption key derivation; gated logic operations and computation assembly vs traditional computation at point of negotiation. The machines use gated logic operations (ie: AND, OR, XOR, NOT) which are native to the structure of computers. These operations use only 1's and 0's to perform all their operations vs using decimal or hexadecimal style mathematics which requires eventual translation to binary mathematics. By using these gated operations, the overhead of translation is almost completely avoided. The machines also store integral components of final keys in their blocks and use a process of assembly at the point of exchange instead of calculation at the point of negotiation/encryption. This method saves overhead versus most if not all encryption methods in use today that require computation of very large numbers and usage of corresponding energy, time and heat to execute (reference 4).

Blockchain Block Formats and Duration

Additional features of the GABED blockchain architecture are the block length, the number of identity type keys and the regeneration interval of the epoch keys. The block length (the number of binary digits) that can be used in each identity key is not limited, this means that increased complexity for attackers can be achieved by dialing up this parameter (we refer to this as vertical scaling). Computational complexity for attackers could be increased by doubling, tripling, quadrupling etc. the size of these identity keys with very little overhead. In addition, due to the small footprint a 50 machine blockchain typically requires 3-4KB storage depending on the number of random epochs generated.

In addition to block length, the number of identity keys can also be varied up in order to require more blockchain knowledge. Finally, the frequency of random interval regeneration of epoch keys can also be controlled through application parameters (not known even to the initial manager tasked with generating the mission blockchain) to force contraction of epochs into more discrete intervals. These simple, incremental parameters can greatly confuse enemy cyber-attacks and provide tamper-resiliency with a very high level of confidence.

Critical Feature: Variability of Content

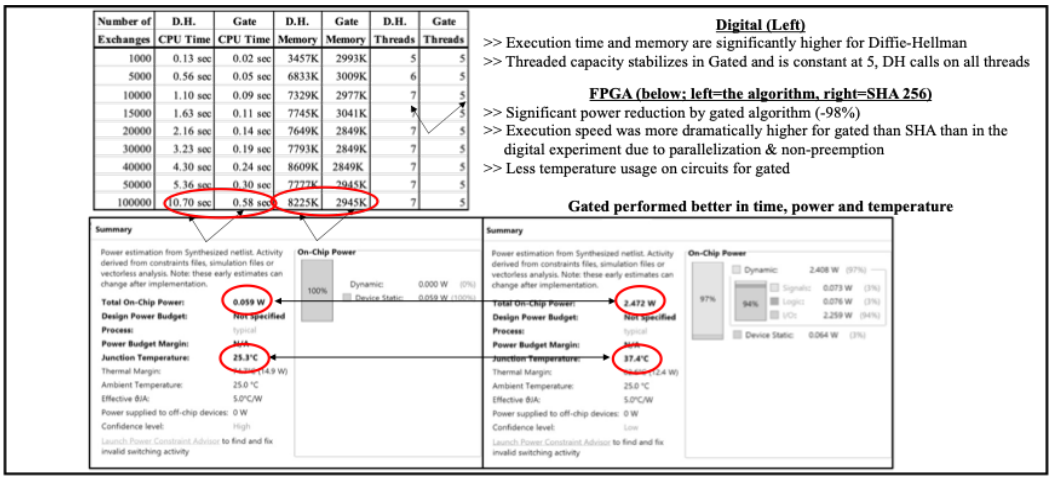


Cumulative Encryption

Internally, the blockchain blocks are encrypted using a specific protocol or method. The GABED blockchain is cumulatively encrypted; all mutations from the beginning of the chain must be known in order to determine the current encryption. A machine must know the encryption used at each epoch and then how it is mutated as the epochs change in order to get the identity keys that are stored in the blockchain. The machine must also know the algorithm for mutation to the next epoch and all successive epochs to know how to un-encrypt the key values for the identities. This cumulative mutational encryption adds an additional layer of security since the entirety of the history and the algorithm must be known in order to produce the 10 keys that are required for value transfer. A main difference in the cumulative encryption versus others like bitcoin is that the GABEDs' encryption and the epoch keys change on random contents at random intervals. Bitcoin uses a method that includes the "nonce" (number used once) and when the number is has been derived then the block can be understood.

Efficiencies in Energy, Time and Heat Dissipation

One key question that might come to mind is how much energy does all this complexity cost? The answer is quite simple, if you have all the inputs, the output is very easy to compute with low energy, speed and heat dissipation. The graphics below are from reference number (4) and depict the comparative advantages of traditional encryption methods (AES/Diffie-Hellman) vs the GABED methods. Significant differences exist in energy usage (around 2/100 for GABED for static + dynamic components, unmeasurable for dynamic since it "just is"; electrons through circuits with no significant logic), speed of computation (20*) and heat (-30%). Items in red indicate the results obtained and published.



Number of Exchanges	D.H. CPU Time	Gate CPU Time	D.H. Memory	Gate Memory	D.H. Threads	Gate Threads
1000	0.13 sec	0.02 sec	3457K	2993K	5	5
5000	0.56 sec	0.05 sec	6833K	3009K	6	5
10000	1.10 sec	0.09 sec	7329K	2977K	7	5
15000	1.63 sec	0.11 sec	7745K	3041K	7	5
20000	2.16 sec	0.14 sec	7649K	2849K	7	5
30000	3.23 sec	0.19 sec	7793K	2849K	7	5
40000	4.30 sec	0.24 sec	8609K	2849K	7	5
50000	5.36 sec	0.30 sec	7727K	2945K	7	5
100000	10.70 sec	0.58 sec	8225K	2945K	7	5

Digital (Left)

>> Execution time and memory are significantly higher for Diffie-Hellman
>> Threaded capacity stabilizes in Gated and is constant at 5, DH calls on all threads

FPGA (below; left=the algorithm, right=SHA 256)

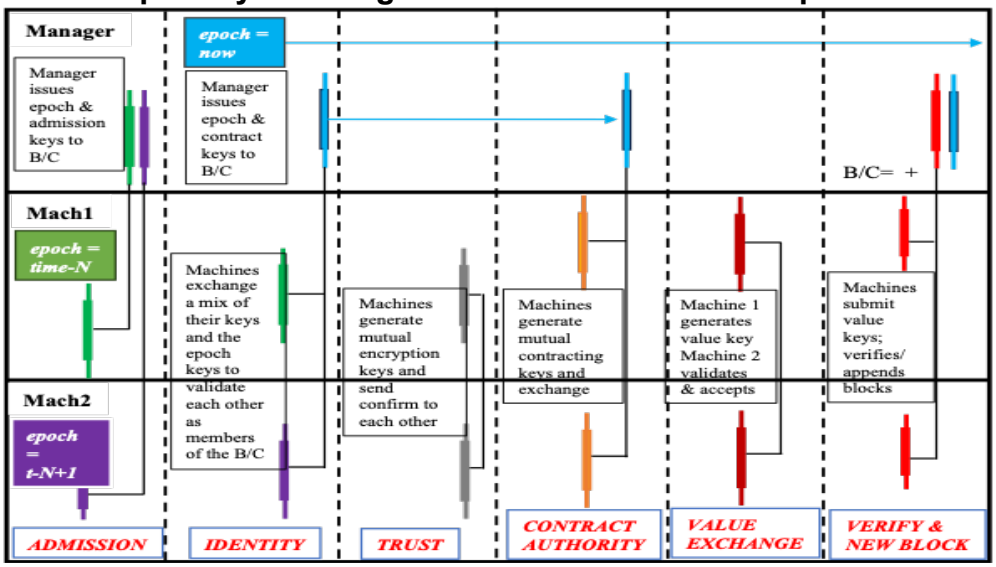
>> Significant power reduction by gated algorithm (-98%)
>> Execution speed was more dramatically higher for gated than SHA than in the digital experiment due to parallelization & non-preemption
>> Less temperature usage on circuits for gated

Gated performed better in time, power and temperature

Shared Intelligence with Zero Trust

Usage of the GABED blockchain network protocol enables the participating devices (GCS, UAS) to share intelligence blocks in an open zero-trust network that is significantly more efficient. As the devices achieve mission tasks, these are shared with other devices and can potentially be used by them in furthering other objectives. This knowledge is critical when independent AI agents are forward deployed in surviving devices to enact new mission objectives. At the minimum level of knowledge, the UAS are able to communicate if they are still alive, but in a fully active environment, the communication protocol enables download of new objectives, plans and coordinates from an AI interface to continue the mission in real time. An example of the theoretical dialogue between devices to establish these abilities is given below (see reference 2):

Sample Key Exchanges in a Transfer of Value Operation



Technical Architecture

The GCS and UAS systems share intelligence on identity, trust and value transfer via their resident blockchains. At the start of the mission, the initial blockchain is generated and distributed to the participants via close Bluetooth communications. Once in flight, the units establish identity and trust through their Blockchain blocks knowledge, GCS units (initially) direct the delivery of the cargo in the cargo bay through specific commands that are negotiated through mutual keys and specialized transactions. Evidence of the payload delivery is taken by duplicate imaging that is shared between the UAS executing the task and its relevant GCS.

This system has undergone two field trials. The first one was conducted in Wallops Island, VA in August of 2025 and proved the ability to have the connectivity for the UAS and the negotiation of keys. The second was executed in North Carolina in September 2025 and proved the ability to communicate to the UAS with multiple RF (from other UAS networks) in the area.

Function/Feature Comparison

#	Criteria	GABEDs	SHA	Ethereum	Comments
1	Identity validation	Y	Y		Both allow for 2 machines to authenticate each other
2	Message encryption	Y	Y		Both allow for messages to be encrypted
3	IoT portability	Y	Y		SHA can be used in IoT but requires programming
4	Hiding attack surface	Y	Y		Both hide attack surface
5	Cyber attack resilient	Y	Y		Both provide common cyber attack resilience
6	Shared intelligence	Y		Y	Both allow for common knowledge between machines (blocks)
7	Consensus	Y		Y	Both allow for consensus in a Byzantine Generals Problem format
8	Transaction ledger	Y		Y	Both provide value transaction ledgers
9	Immutability	Y		Y	Both provide immutability of blocks
10	Block encryption	Y		Y	Both provide encryption of blocks into the blockchain
11	Decrease of attack surface over time	Y			As more epochs are appended, attackers face more challenges
12	Variable length keys	Y			Gabeds can vary in key length even within the same epoch
13	Random time-driven regeneration of parameters	Y			Gabeds regenerate at epoch change
14	Efficient computation	Y			Gabeds use blocks and xors to compute
15	Speed of computation	Y			1/200th of time required to process authentication than SHA 256
16	Power effiiency	Y			Gabeds use 1/1,000th++ less energy
17	Temperature efficiency	Y			Gabeds are 1/3 temperature efficient
18	Portability to different processing architectures	Y			Gabeds can exist in circuitry and others
19	Able to retrofit older architectures	Y			Needs available gates (10K) and some firmware enhancements
20	Does not require additional software	Y			Requires standard digital logic operations on gated arrays
21	Quantum resilient	Y			Due to randomness, Gabeds can be quantum resistant

SHA refers to the family of algorithms commonly used to shared information with known entities in encrypted mode. AES 256 is the most common however, there is a strong recommendation to implement AES 512 (512-bit keys). **Ethereum** is a leading software package providing blockchain functionality out-of-the box.

Enhancing Protection Provided by UAS Radios

Our clients have frequently asked, is the AES-256 (typically) protection in radios not sufficient in order to protect the UAS? In our opinion, radios tend to solve link protection (anti-jam, anti-intercept), spectrum resilience and data-in-transit security. On the other hand, GABEDs address different unprotected areas:

- Device identity (is this UAS/authentic component trusted?)
- Data integrity at origin (can the data itself be trusted?)
- Protection against spoofing, cloning, and supply chain compromise
- Secure coordination across multiple autonomous systems

In highly hazardous situations, most successful attacks are not breaking AES encryption. However, they are GPS spoofing, impersonating devices, injecting signals and may have compromised hardware that can be hacked by electronic signals. In those situations more protection is recommended to avoid:

- Adversaries bypassing encryption—not cracking it
- Autonomy + AI increases consequences of bad data (it is a new attack surface)
- Swarm operations require trusted device-to-device communication.

In our opinion, the question should be: "*Can we trust the device and the data at all?*" instead of "Can someone read the signal?"

The new areas of focus are mission assurance over unit cost, survivability in contested environments and compliance with emerging US DoW security frameworks. Our clients are sensitive to CPU constraints, power budgets and pushback on AI hardware tradeoffs required. In these cases, GABEDs offer to minimize onboard compute burden, a lightweight hardware-rooted identity layer and integration alongside existing radios (without replacing them).

CONCLUSION

The emergence of quality, low-cost unmanned systems presents a tremendous opportunity for leadership in the new landscape of national defense and continued effort to overmatch enemies through unparalleled coordination of military platforms. By further enhancing cyber security and providing native shared intelligence, defense efforts can defeat enemy cyber operations to attack and neutralize a wide range of platforms. GABEDs is prepared to provide the needed level of security at speeds and computational ability for this and future generations of conflict.

REFERENCES

1) "Generation, regeneration and validation of binary secret keys through blockchain in IoT devices" https://www.athensjournals.gr/sciences/2022-9-1-2-Medellin.pdf
2) "Scalability and Cyber Resilience in Gated Array Blockchain Enabled Devices" https://www.athensjournals.gr/technology/2025-6502-AJTE-COM-Medellin-05.pdf
3) "Device For Implementing Gated Array Blockchain Protection Codes For IoT Devices" US Patent Number 12549389 Issued February 10, 2026. USPTO.
4) "Exploiting Efficiencies in IoT Key Exchanges Through Reversible Logic Blockchains" https://link.springer.com/chapter/10.1007/978-3-031-92625-9_13#:~:text=The%20FPGA%20(Field%20Programmable%20Gated,resources%20need%20to%20be%20conserved.

5) Free access to #4 above: https://mede-arc.com/pubs%2Fvitae

CONTACTS

John M. Medellin, PhD, CPA
john@mede-arc.com
ph: 1-214-244-4095

Mia Guinan (Public Sector)
mia@guinangroup.com
ph: 1-757-617-0033

Frank Sandoval (Private Sector)
frank@sarglostrat.com
ph: 1-832-692-3441