VeroGuard Systems

VeroGuard & Blockchain Opportunities

Addressing Blockchains issues with Identity, Security and Scalability

The Problem

Blockchains have several major barriers that make them impractical for mainstream use today. VeroGuard can accelerate blockchain commercialisation by helping to address some of the key issues of Identity and Security, and could also realise benefits with Scalability, Privacy, Formal Contracts and reduce Storage requirements.

Blockchain and VeroGuard

While blockchain technology can be used in different ways, a blockchain solution generally builds on four features.

1. **Decentralized validation.** When a transaction such as a ticket sale occurs, new data blocks describing it are added to a chain only after consensus is reached among the relevant participants on the validity of the action—for example, when the seller is validated as the owner of a ticket that is sold.
2. **Redundancy.** The blockchain is continuously replicated on all or at least a group of nodes in a network. As a result, no single point of failure exists.
3. **Immutable storage.** Blockchain confounds hackers because to tamper with data they would have to alter not just one block in a chain but also all successive blocks and the majority of their replications. In addition, data is registered in the blockchain with a digital fingerprint that includes a date and time stamp; any attempt to change data would be apparent because the new digital fingerprint would not match the old one.
4. **Encryption**. Digital signatures based on pairs of cryptographic private and public keys enable network participants to authenticate which participant owns an asset, initiated a transaction, signed a smart contract, or registered data in the blockchain.

Blockchains have several major barriers that make them impractical for mainstream use today.

Whilst most of the significant and well documented issues with blockchain centre around scalability, security, standardisation and regulation the various blockchain research and development are focused on trying to resolve a number of challenges including:

1. Limited scalability - While a decentralization consensus mechanism offers us the core benefits of blockchain that we all care about — security guarantees, political neutrality, censorship resistance, etc. — it comes at the cost of scalability, since decentralization by definition limits the number of transactions the blockchain can process to the limitations of a single fully participating node in the network. Two practical implications here:
    - Low throughput: Blockchains can only process a limited number of transactions
    - Slow transaction times: The time required to process a block of transactions is slow. “Right now, Ethereum can process 17 transactions per second. Facebook can handle 175,000 requests per second. Visa, 44,000 transactions per second. So, if we really want to use cryptocurrencies as currencies, it would not be possible as of this moment.”
2. Limited privacy - Given that blockchain transactions are not tied directly to your identity, they may appear more private. Anyone in the world can create a new wallet anonymously and transact using it. Paradoxically the appearance of total anonymity is misleading. It’s true that a person can preserve his or her privacy as long as the pseudonym is not linked to the individual, but as soon as somebody makes the connection, the secret is revealed. Uploading critical business data into a blockchain where hackers, competitors, or other unauthorized parties can view the information is simply not an option for most companies. Consider:
    - **Electronic medical records**, which are extremely private and sensitive information. It’s unacceptable to ever have that information publicly visible on public blockchains, thereby jeopardizing patient confidentiality.
    - **Identity verification data** such as social security numbers cannot be openly stored in a public smart contract.
    - **Credential management** such as passwords and keys have no place in an open, ultimately unsecured smart contract.
    - **Financial documents** such as e capitalization tables or employee salaries should never be publicly associated with addresses that are easily traceable.
3. Lack of formal contract – verification of smart contracts remains a HUGE unsolved problem. Smart contracts are immutable, meaning you can’t update or fix them once they’ve been deployed onto the main Ethereum network. Everything needs to be exactly right before deploying contracts in real-world applications. Moreover, smart contracts are publicly accessible and anything stored within smart contracts is open for anyone to view; anyone can also call into the public methods of smart contracts. While this provides openness and transparency, it also makes smart contracts very attractive targets for hackers.
4. Storage constraints - Most applications that get built on a public blockchain will require some sort of storage solution. (User identities, financial information, etc.). However, storing information on a public blockchain database means that the data is:

- Stored by every full node in the network.
- Stored indefinitely since the blockchain database is append only and immutable.

Therefore, data storage imposes a huge cost on a decentralized network where every full node has to store more and more data into infinity. As a result, storage remains a huge hurdle for any realistic application that gets built on the blockchain

5. Unsustainable consensus mechanisms – Current mechanism's for 'proof of stake' or 'proof of work' have not shown an ability to be resource efficient or able to avoid oligopolistic chains.
6. Lack of governance and standards - **there literally is no safe upgrade path for the protocol, and no one responsible for setting and maintaining standards.** While we definitely want to keep the development of blockchain technology as decentralized as possible, we still need some organisation amongst developers and others in the ecosystem to agree on new standards, features and upgrades. It's unclear how you achieve this without leading to at least some centralisation (e.g. The Ethereum Foundation).
7. Inadequate tooling - I**t goes without saying that the developer tooling currently available for the blockchain ecosystem is unacceptable.** Developing a functional protocol or decentralized application on the blockchain is a daunting task even for today's most seasoned developers. This is another major issue for blockchain development, lacking suitable debugging tools, compilers, deployment tools, testing frameworks, documentation, logging tools, security auditing and analytics leaves blockchain a very inefficient and ineffective platform also vulnerable to weaknesses in security and reliability.
8. Lack of an Identity layer - Because the Internet currently misses a native identity layer, companies and public institutions have implemented an ad-hoc system of workaround like internal databases– incompatible data silos in which they then manage the identities of people and things in their data ecosystem. Problems that arise from these data silos:
    - It is expensive to maintain security of identity data (theft or loss of data)
    - Data compatibility with other institutions comes at a high cost.
    - Users have no control of their data and do not know when it is passed on to other institutions
    - Users waste a lot of time creating and managing multiple usernames for a single app or new service they register for.
    - No control over their own data: The user doesn't have a consolidated digital identity, but rather tens or hundreds of fragments of themselves scattered across different organizations, with no ability to control, update or secure these fragmented identities effectively.
    - Fraud: (a) Companies cannot uniquely identify bad actors that might order goods they never pay for; (b) Users might be paying for goods or services online that they never receive.

Blockchain-based transactions across jurisdictions will face these same problems, and as agreements become auto enforceable and entries in the database immutable, these problems may become even worse.

How can VeroGuard enable rapid blockchain deployment?

Significant activity in the market is being made to address a number of these issues however a clear breakthrough on governance, scale, security and conformity remain largely theoretical.

VeroGuard provides a ready to integrate solution that can accelerate blockchain commercialisation by helping to address some of the key issues:

Importantly and initially VeroGuard can work to apply:

1. Identity: VeroGuard can provide non-repudiable identity to any actor in blockchain development. With verifiable identity more rapid implementation of both private and public blockchains could be achieved by providing greater trust, easier proof of stake speedier verification of source with improved privacy and control over entries.
2. Security: VeroGuard verifies the actors in transactions and can stamp every entry with the source. Further hash's can be protected and even backed up in VeroGuard's unique system removing the risks and threats that are commonly manifesting themselves in cryptocurrencies at the moment (loss and theft of currency).

VeroGuard believes development work could also realise benefits with:

1. Scalability: By verifying actors as non-repudiable identities in networks, an opportunity exists to accelerate and strengthen Delegated Proof of Stake to reduce resource requirements in networks radically increasing the capacity to speed networks.
2. Privacy: VeroGuard can immediately provide privacy and protection for any data in the distributed ledgers by only allowing verified parties to access, and the capability to overlay VeroVault for data protection.

3. Formal Contracts: VeroGuard can leverage its cryptography to apply immediate verifiable, immutable smart contracts to accelerate other specific elements of blockchain to be implemented.
4. Storage constraints:
    - Improved verification of source information and blockchain actors combined with delegated proof of stake has the chance of delivering a solution that is significantly less resource hungry.
    - Possibility to create a global storage solution with VeroVault and Data61 for blocks to allow a high performing, ultra-secure fast integration and interaction environment to simplify and reduce costs of commercial applications.

What other reasons are there to accelerate and hybrid blockchain solutions.

1. Realising potential of Blockchain
    - "When I talk to people who really understand what blockchain-based technology is about, they will quite openly say we're talking about 10- to 20-year time frames here," says Martha Bennett, a principal analyst with Forrester who has been studying the area for three years."[1] **By resolving some of the most significant issues with blockchain now, disruptive commercial applications utilising the benefits of immutable ledgers can be implemented in the near term..**
2. Unification of identity.
    - The direct economic benefit of unifying digital identity and finding commercial applications for blockchain are significant. A Boston Consulting Report shows that the potential value created through just an implementation of a unified digital identity can indeed be massive: €1 trillion in Europe by 2020, or roughly 8 percent of the combined GDP of the EU-27.
3. Cyber Crime fastest growing crime in the world.
    - Forbes estimates that the economic impact of cyber crime will increase 600% from 2017 to 2021 to over $US6 trillion per annum, or about 8% of global GDP. Current approaches to detecting cyber crime rather than stopping it and the associated fraud are not currently stemming the tide. Attempts to anchor an identity to a biometric have proven to be massively exposed to technical complexity, fraud and identity crimes. Blockchain with Vero could provide a significant opportunity to greatly reduce risk of data loss and online fraud.
4. Government have an opportunity to open markets and lower the cost of doing business
    - Digital infrastructure needs to be improved to help businesses engage safely online and reduce effort to work online.

[1] https://www.databreachtoday.com/blockchain-for-identity-management-its-years-away-a-10598

References:

The 5 big problems with blockchain everyone should be aware of - Forbes
https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/2/#4c79070d67bc

The Truth about blockchain - Harvard Business Review
https://hbr.org/2017/01/the-truth-about-blockchain

Key Challenges Blockchain
https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-key-challenges.pdf

Fundamental challenges with public blockchains
https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428

Before crypto nirvana, blockchain needs to solve these basic problems
https://www.digitaltrends.com/computing/blockchain-problems-how-to-solve-issues-with-the-latest-vogue-tech/

Blockchain may power future elections, but it's no silver bullet for fraud
https://www.digitaltrends.com/computing/blockchain-could-be-implemented-in-electoral-voting-by-2019/

VeroGuard Systems Pty Ltd
ABN 25 617 573 001

P / +61 (03) 9558 3090
admin@veroguard.com.au

veroguard.com.au