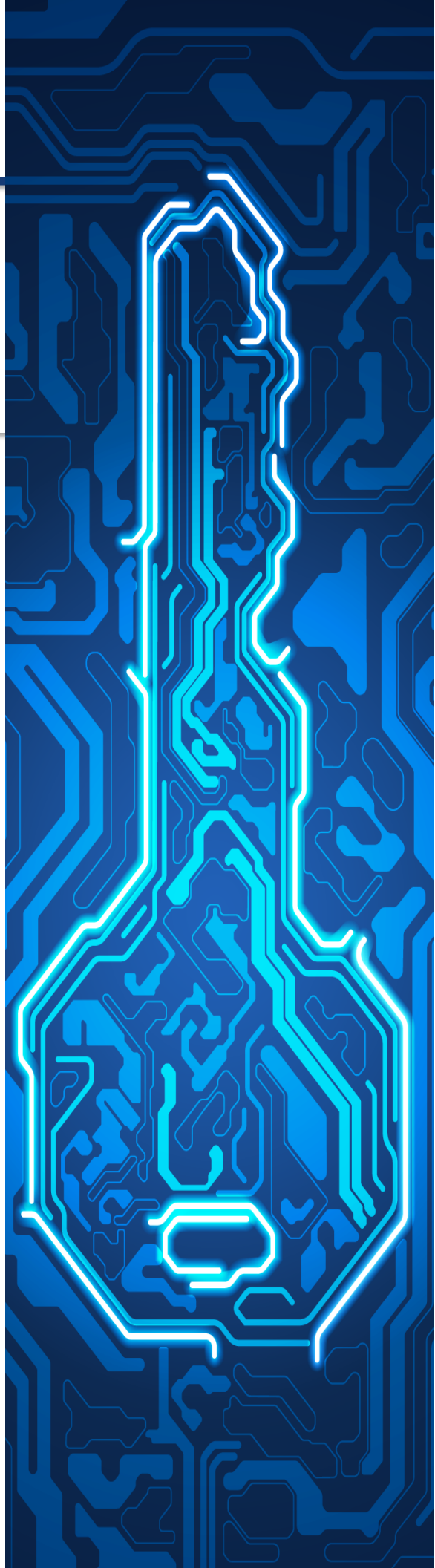
Integra

Briefing Note

BLOCKCHAINS AND WILDLIFE TRAFFICKING

Advanced Tools to Address Corruption and Fraud



Blockchain technology has risen in profile and prominence in recent years, driven in large part by the rise in Bitcoin and other cryptocurrencies. At its most basic, it is an open accounting technology that can record transactions between two parties efficiently and in a verifiable and permanent way. As mundane as this is, it is also a disruptive technology poised to transform how business is done. It is transforming the global economy, yet is still not understood well by governments, companies and citizens. If misused, blockchains can be a mechanism for bad actors, for example, by facilitating money laundering or trafficking. If used well, however, blockchains can also have substantial benefits in fighting crime. They can, for example, defeat money laundering through permissioned networks where participation is conditional on verified identity, and corruption by making forged documentation impossible.

To ensure that blockchains remain a force for good, governments need to keep better pace with technological developments and put in place the right enabling environment to support their effective use. There is also an imperative to focus blockchains on transparency and to use the technology to defeat financial crime and corruption.

This briefing note explains the basic blockchain concept and its potential legitimate and illegitimate uses, with examples of applications for combating wildlife trafficking. Some policy options are identified, including simple processes such as using blockchains to secure important documents relating to certification of origin or of sustainable production.

John Waugh, Vice President, **Integra LLC**

jwaugh@integrallc.com
1110 Vermont Ave NW, Suite 750 ■ Washington DC 20005 USA
+1 202 898-4110 ■ www.integrallc.com

What is a blockchain?

The easiest way to explain the concept of a blockchain is to think of it as an accounting technology. It is a distributed digital ledger, or way of tracking assets, both tangible (e.g., car, or a plot of land) and intangible (e.g., certifications, passports, driving licenses). At the same time, the blockchain concept can be thought of as an "operating system" for a distributed network.

Double-entry accounting has been the universal operating system of markets for the past 600 years. It provides agreed standards and protocols for describing assets (debits and credits). This system produces a record of aggregated value. But it is static and inefficient; each party to a transaction keeps their own record, and these have to be reconciled and audited, which is time consuming and expensive. And double-entry accounting can be manipulated to hide assets or debt.

The blockchain is the "next generation" operating system for global accounting. What is new is that the transaction record is shared and available to all the parties. This record is why some call the blockchain a "triple-entry" accounting system.

The blockchain ledger is dynamic, capable of recording huge numbers of transactions in real time. Its components are:

1. **The Network of Computers Participating in the Blockchain**
   Each participant in the network acts as both a publisher and a subscriber, providing peer-to-peer replication. Because the network is constantly checking itself, and because the blockchain is distributed across a network, multiple encrypted copies of each record exist. Even if someone manages to break into a block, any alterations they make would be obvious; anyone can verify a transaction by comparison with the other records, so the provenance and accuracy of the data is assured.

2. **The Records of Transactions Known as "Blocks"**
   They contain a "hash", a unique identifier and are time-stamped.

3. **A Chain of Blocks, which Encodes the History of each Record**
   They provide a record of the provenance and chain of custody. This makes it possible for the parties to a transaction to agree on a specific interpretation of reality.

4. **Smart Contracts**
   That stores the rules governing a transaction, or terms of the contract in the blockchain code. Transactions are traceable and immutable, and some may have clauses that are self-executing.

A major constraint to the adoption of blockchain technologies is that the legal framework regulating contracts and other transactions will require amendment to accommodate the new technology and many of its uses. Systems for reporting, auditing and taxation will need to be overhauled. Business is already making the transition, and blockchains, for better or worse, may make much of the regulatory framework worldwide obsolete.

"The Blockchain is like a book. The pages are numbered; the . . . entries are immutable. The book is published and all people can see it. Since it is stored in many places at the same time and no single place can control all nodes, one will not be able to convince the world of a fake version of the truth."

- *Michael Taverner,* ***Bitfury***

What are the benefits of blockchains?

- **Provenance.** The blockchain is time-stamped and complete, it tells how and when a transaction has taken place. Imagine a title for an automobile that includes all the previous owners, and its entire repair history.
- **Immutability.** The distributed record has to be reconciled with all other versions to be valid; so, it is unalterable – the only way to change it is to record a new transaction.
- **Completeness.** Because any transactions recorded convey with the record, a blockchain provides the last word, expediting auditing and monitoring. The blockchain is self-regulating.
- **Transparency.** Blockchains can make business processes such as shipping and inventory more visible, allowing for improvements in logistics and in forecasting. The status of assets can be monitored in near real time.
- **Control.** In "permissioned networks", participation is restricted to authorized parties determined by a "certificate authority". In a permissioned network, users can set levels of access to their information in order to control who can view a record.
- **Automation.** Transactions can be recorded, monitored, and verified much quicker, compliance with regulations confirmed – reducing regulatory burden.

What are the uses of blockchains?

A blockchain is used to enhance accountability. It creates confidence that otherwise could not exist in the provenance of items being accounted; it also creates security in transactions by verifying ownership, transfer of title, etc. Security and transparency produce the possibility of trust.

They work well in situations with multiple parties that need to participate in a system. One example is a supply chain. For example, a blockchain could validate the provenance of certified palm oil or biofuel. In a more complex system, like aircraft parts, where the authenticity of parts is of paramount importance, the chain of custody of an individual part can be traced from manufacture to deployment.

The most prominent application of a blockchain is Bitcoin, a type of cryptocurrency. Many people think that Bitcoin and blockchain are the same things. Blockchain is actually the technology that Bitcoin uses. The high level of trust in blockchain transactions is what makes cryptocurrency possible.

E-government is another example of a blockchain application. In 2017 the Republic of Georgia made history when it announced that it was converting its land administration to a blockchain based system for recording titles and liens. Georgia had a history of state corruption, and land transactions provided an easy target for corrupt officials. Its reform-minded government intends to stamp out forgery and duplication using blockchain technology. Sweden, Canada, and Australia are following suit, because, in addition to enhanced security, the process is more efficient. It will reduce the costs of administration and reap the benefits of digital data management across government, which will result in more efficient and evidence-based services.

The 2017 presidential election in Sierra Leone attracted attention because of a blockchain experiment in tabulating votes. The Swiss foundation Agora, as an independent observer to the election, created a tally using a blockchain from 20 polling stations, and published the results online, allowing cross checking with the official tally of the National Election Commission.

Of course, voting data is only as secure as the initial entry, the vote being cast. Further security measures can be achieved when the entire system, including voter registration, is secured with a blockchain.

In the future, blockchains will enable more secure identification to thwart fraud in health care, insurance, and financial transactions. Forms of identification, such as passports and birth certificates, will be made tamperproof as well.

Can criminals exploit blockchains?

The Silk Road dark web site, an anonymous marketplace for the exchange of almost anything, including contraband, ran on blockchain technology for financial transactions, using cryptocurrency for more than one billion dollars in transaction. "Dark market" exchanges constitute a small percentage of cryptocurrency use. There is concern however that smart contracts can facilitate money-laundering because of the decentralized process. Financial regulation is one reason that smart contracts aren't already mainstreamed. Most cryptocurrencies are subject to regulatory requirements. Requirements of positive identification of customers by banks for example, means that there would need to be some positive way to identify participants, e.g. by biometric means.

Even so, Bitcoin is not truly anonymous, and transactions can be monitored by law enforcement. Silk Road was brought down by software by payments tracked through the blockchain ledger. In response, criminal networks are drawn towards more black-market (unregulated) cryptocurrency variants called "altcoins" offering advanced privacy features. These use "zero-proof technology" to strip out identifying information from the ledger.

Another strategy for avoiding law enforcement is the use of the basic tool of the "dark web", the Onion (or Tor) router, which anonymizes user IP addresses. Blockchain is thus evolving to become untraceable.

Blockchains is used for extortion, as has been seen recently by ransomware exploits that demand payment in cryptocurrency. Cryptocurrency is also being used for tax evasion and contraband transactions.

How Is law enforcement using blockchains?

A major weakness of cryptocurrency is that it can't be readily exchanged for most goods and services, except in risky unregulated exchanges. Where cryptocurrency is converted to other assets like money or goods, it is vulnerable to observation. Law enforcement can monitor liquidity movements within and between blockchains to detect patterns and anomalies, tools already in use in combating financial crime. Patterns can help to "de-anonymize" transactions. This approach brought down the Silk Road dark web trading system (apparently implicating undercover law enforcement agents gone rogue along the way).

Blockchain technology can also be used by law enforcement for its own integrated, decentralized monitoring of financial transactions. This would require the participation of the entire financial system. The benefit would be that suspicious activity can be highlighted and distributed to law enforcement throughout the system.

Trust in sharing of sensitive information between law enforcement agencies is a barrier to more effective cooperation, especially in the case of transnational criminal networks. If law enforcement records were encrypted and distributed within a permissioned network using blockchain technology across departments, agencies and/or regions, it would produce a system with vast amounts of data that would be impenetrable to hackers and would protect the identify and behaviors of members of the network. Users could specify controls on who can access their data, and under what conditions. This would

put actionable intelligence in the hands of users without compromising the security of investigations. When combined with machine learning tools, it could detect invisible patterns.

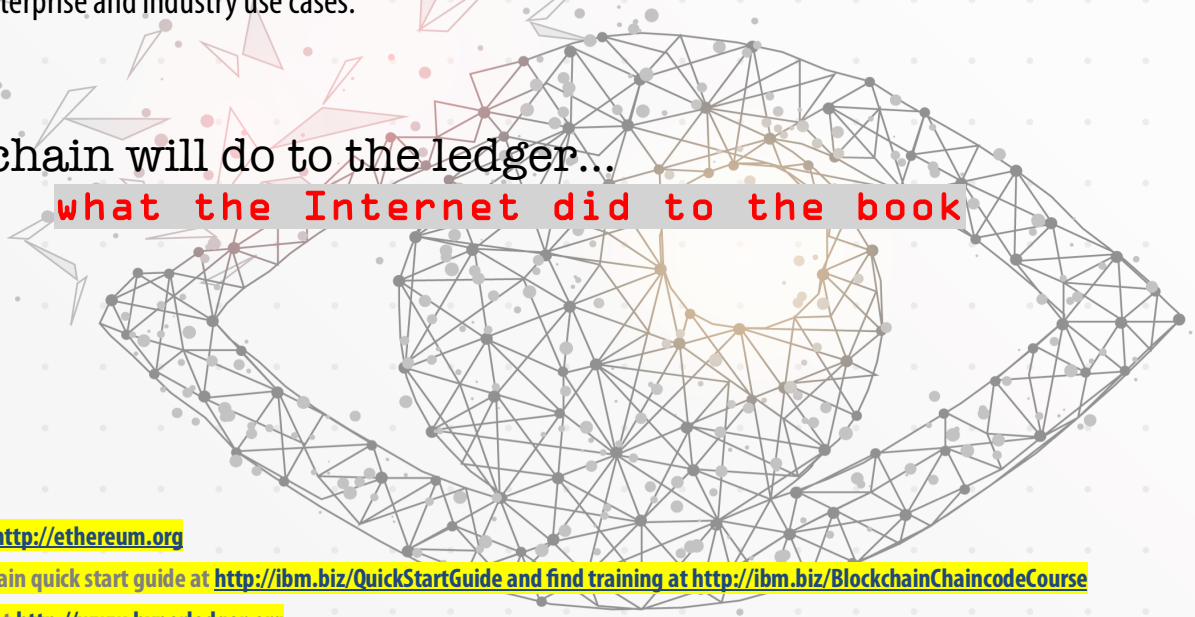
Customs officials can benefit from blockchain based supply chain and logistics tools to better monitor for possible contraband in cargos through permissions extended to regulators.

How to begin using blockchain to combat wildlife trafficking

The first step is to understand the principles and tools for blockchains. Because humans write code, smart contracts are only as good as their developers. Building blockchain applications from scratch requires significant coding and cryptography skills. However, a number of open source platforms have emerged to simplify the process of developing blockchain based applications. While it is still necessary to have core competencies to produce good products, these platforms allow developers to produce customized, decentralized applications (dapps) by building on top of existing open-source products. There are dapps for much of the functionality described in this briefing note. For example, there are prediction and forecasting market dapps, as well as dapps for tracing provenance in supply chains.

One of the leading platforms is Ethereum. The Ethereum Virtual Machine enables developers to produce an unlimited number of dapps that run on its blockchain network. Dapps are made up of code that is not controlled by a central entity. With Ethereum, a developer can also build Decentralized Autonomous Organizations, or DAOs. DAOs are run by a collection of smart contracts on the Ethereum blockchain. The code replaces the rules and structures of a conventional organization, eliminating the need for central control (e.g., a "secretariat"), yet allow the organization to operate transparently. Ethereum charges transaction fees in the form of its own cryptocurrency, Ether. It is possible however to build private (permissioned) blockchains.

Hyperledger is a Linux Foundation project to support the open source software development community. Its approach is to facilitate the development of a wider range of platforms and modules focused on distributed ledger and smart contract technology. Technology giants like Intel and IBM are producing and distributing software through Hyperledger. Unlike the single platform of Ethereum, Hyperledger is an open standard on the model of Apache server software, which allows new blockchain stacks to be created. Hyperledger is advantageous for the development of permissioned blockchains, and its focus is on the business enterprise and industry use cases.



References:

Visit Ethereum at http://ethereum.org

Visit IBM's blockchain quick start guide at http://ibm.biz/QuickStartGuide and find training at http://ibm.biz/BlockchainChaincodeCourse

Visit Hyperledger at http://www.hyperledger.org

Explore dapps at http://ww.stateofthedapps.com

Methods for combating wildlife trafficking

Use cases for CWT blockchains include needs for provenance, certification of authenticity, and secure information exchange.

- **Provenance.** In supply chains, blockchains can ensure a secure and immutable record of the chain of custody of a wildlife product, making it possible to distinguish legal wildlife products using a registration system. For example, smart contracts for timber that certify provenance would vastly strengthen the traceability and therefore the confidence in the authenticity and source of the item being certified. This can also be applied to regulate minerals, which can otherwise be sourced from illegal production (e.g., "conflict diamonds), or production in protected areas (e.g., artisanal gold from wildcat mines in the eastern DRC).
- **Certification.** In regulation, blockchains can be used to secure official permissions, such as the CITES export certificate. If the CITES Secretariat was the certificate authority, and national CITES authorities were the blockchain nodes in a permissioned network, this would strictly limited access to export certificates, eliminating the possibility of a forged or fraudulently altered certificate.
- **Secure Information Exchange.** A wildlife enforcement network could adopt a DAO, in order to share privileged information securely.

RECOMMENDATIONS

- **Commerce**. Blockchain technologies can be used in Southeast Asia to facilitate trade logistics while improving monitoring, to share information within a trust network, and to improve confidence in certifications of sustainable production and legal compliance.
- **Law**. Law has not kept up with technology, and blockchains operate in a grey area where transactions that are prohibited by law cannot be easily enforced. It is possible, for example, to hide non-transactional data in the chain. Researchers have discovered contraband such as child pornography in the Bitcoin blockchain. Technically, if that is the case, anyone hosting a node would be in violation of the law in many countries. Some analysts believe that the full force of the law will kill blockchains. Others feel that blockchains will not be eliminated, and may gradually erode government control of many functions, such as adjudicating contracts. This is an issue that is bigger than wildlife crime, and it should be borne in mind that blockchains provide tools to improve government, even as it disrupts the existing system.
- **Institutions**. Some uses of blockchains will require political consensus and cannot be decided at the program level (e.g., ASEAN or CITES). In order to advance down the road to more secure transactions, proofs of concept are required. Ideally a use case can be found where the absence or dysfunction of a central authority is a barrier to supply chain transparency. Preventing fraud in the issuance of CITES certificates for example may eventually be possible through the use of a blockchain. In order for this to happen, some robust proofs of concept should be demonstrated.
- **Regulations**. The tremendous cost savings realized by the financial services sector will make blockchains irresistible, but this sector will not tolerate competition from unregulated free-riders. Whether it is possible to stamp out black market blockchains is a subject of considerable debate. It is inevitable though that some forms of regulation will come to blockchains. What is important is that the conservation and law enforcement communities be prepared.

They should work together to examine issues and options for effective regulation of trafficking in contraband of all forms in public forums, and draft regulations to have at the ready when lawmakers move on this issue.

- **Practical proofs of concept**. The point of a proof of concept is to start small and demonstrate that smart contracts and transparency in supply chains using blockchains is feasible and builds the comfort of stakeholders in the new technology. For example, some wildlife and wild-caught fish products in the ASEAN region that are now regulated could be made traceable using blockchain technologies, which would help to differentiate products from legal and illegal sources.[1]

[1] Another opportunity to use a blockchains for a proof of concept in the broader world of natural resource management would be in the labeling of sustainably produced products. For example, it may be possible to develop a pilot activity in partnership with the Forest Stewardship Council or with a Voluntary Partnership Agreement under the European Union's Forest Law Enforcement, Governance, and Trade Action Plan, to ensure provenance of certified or legally harvested timber. Yet another option would be a no-deforestation, no peat, and no exploitation certification for palm oil (perhaps in combination with a USAID activity such as LESTARI (Indonesia) or Green Invest Asia (SE Asia regional)