NELSON MULLINS

FinTech University

FinTech and Health Care
December 5, 2023

Agenda

- Application of FinTech in Healthcare
- Benefits and Challenges
- Emerging FinTech-Healthcare Landscape
- Future Trends
- FCA litigation after cyberbreach
- Blockchain Technology in Health Care

Benefits of FinTech in Healthcare

- Why FinTech in Healthcare?
- Growing role of FinTech in Health Care
- Health Care as % GDP
- Access to Care
- Price Transparency
- Complexity of Medical Billing
- Timely payments
- Medicaid Expiration
- Bridging the Gap between Finance and Health
- Venture capital flooding into FinTech

FinTech Applications in Health Care

- Digital Payment Solutions
- Health Insurance Technologies
- Healthcare Savings and Investment Platforms
- Telemedicine and Virtual Health Services
- Electronic Health Records (EHR) Management

FinTech Applications in Health Care

- Digital Payment Solutions
- Health Insurance Technologies
- Healthcare Savings and Investment Platforms
- Telemedicine and Virtual Health Services
- Electronic Health Records (EHR) Management

Benefits of FinTech in Health Care

- Improved Access to Care
- Cost Reduction and Efficiency
- Personalized Financial Planning
- Data Analytics for Better Healthcare Decision-Making

Challenges of FinTech in Healthcare

- Data Security and Privacy Concerns
- Regulatory Compliance
- Adoption Barriers
- Digital Divide

Future Trends

- Artificial Intelligence and Machine Learning
- Blockchain for Data Security
- Wearable Health-Tech Devices
- Personalized Health Financing
- Regulatory Changes
- Cybersecurity – DOJ Civil Cyber Fraud Initiative

DOJ Civil Cyber Fraud Initiative

- Goal: Hold accountable entities or individuals that put U.S. information or systems at risk by knowingly:
- Providing deficient cybersecurity products or services
- Misrepresenting their cybersecurity practices or protocols
- Violating obligations to monitor and report cybersecurity incidents and breaches
- FCA applicable through flow of CMS dollars
- Emerging trend amongst FCA Relators' Counsel
- Jelly Bean case - $300,000 FCA Settlement
- Aeronet case - $9 million FCA Settlement

Blockchain Technology

- Blockchain is a peer-to-peer (P2P) distributed ledger technology for a new generation of applications that establishes transparency and trust.
- Blockchain consists of three main components: a distributed network, a shared ledger and digital transactions.
- The funding backdrop is healthy and the eco-system is growing.
- Once considered the technology behind Bitcoin, this technology has taken center stage from its crypto-currency roots.
- Blockchain is a means of recording and verifying data in a tamper and revision-proof way that is public to all.

Blockchain Technology

Distributed Network

- Blockchain is a decentralized P2P architecture with nodes consisting of network participants.
- Each member in the network stores an identical copy of the blockchain and contributes to the collective process of validating and certifying digital transactions for the network.

Shared Ledger

- Members in the distributed network record digital transactions into a shared ledger.
- To add transactions, members in the network run algorithms to evaluate and verify the proposed transaction.
- If a majority of the members in the network agree that the transaction is valid, the new transaction is added to the shared ledger.

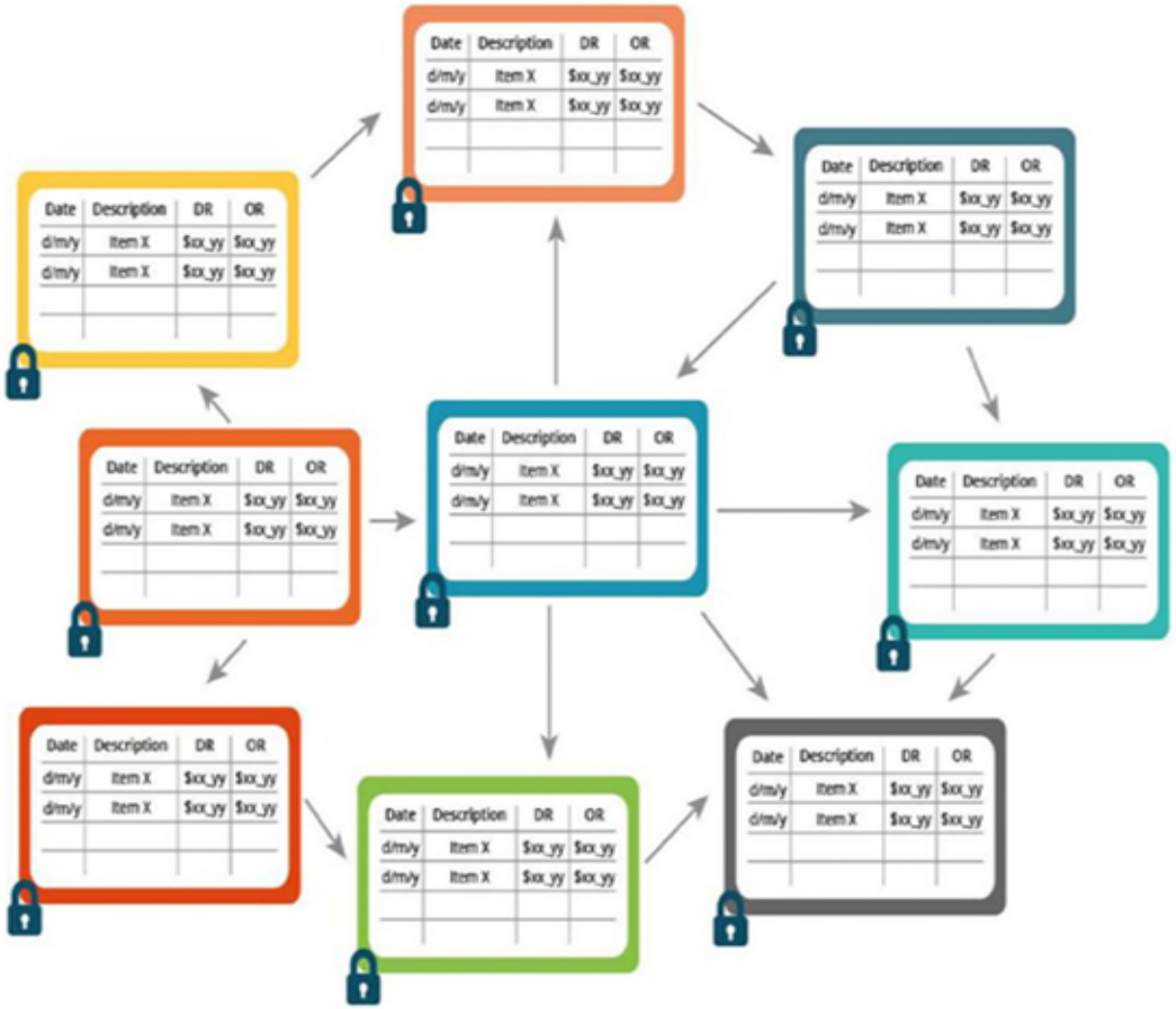
Blockchain Technology

- Changes to the shared ledger are reflected in all copies of the blockchain in minutes or, in some cases, seconds.
- After a transaction is added it is immutable and cannot be changed or removed.
- Since all members in the network have a complete copy of the blockchain no single member has the power to tamper or alter data.

Digital Transactions

- Any type of information or digital asset can be stored in a blockchain, and the network implementing the blockchain defines the type of information contained in the transaction. Information is encrypted and digitally signed to guarantee authenticity and accuracy.
- Transactions are structured into blocks and each block contains a cryptographic hash to the prior block in the blockchain. Blocks are added in a linear, chronological order.

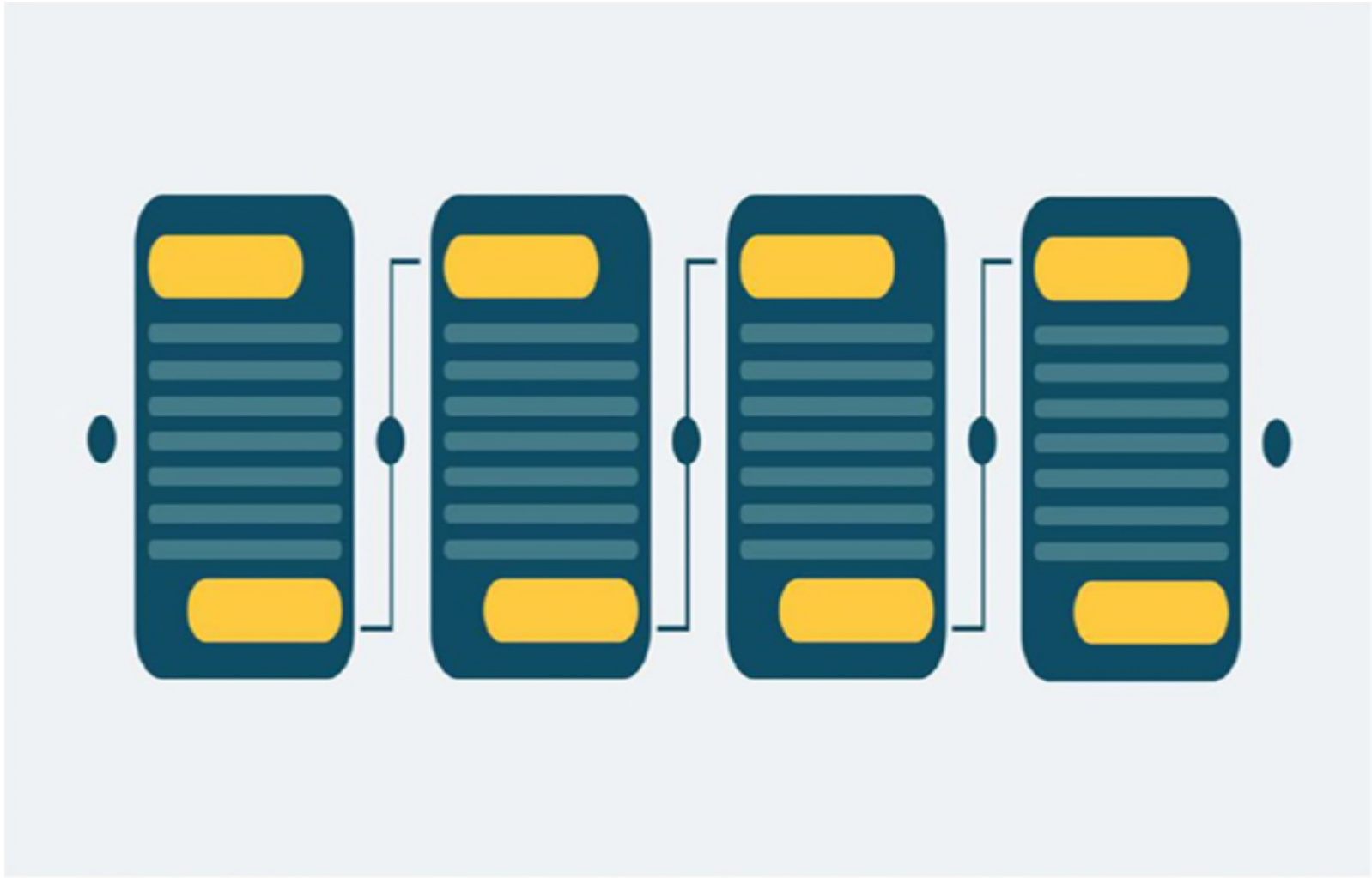
Blockchain Technology



Blockchain is a decentralized P2P architecture. Members in the distributed network record digital transactions into a shared ledger. Each member stores an identical copy of the shared ledger and changes to the shared ledger are reflected in all copies.

Source: Laura A Linn, Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research

Encryption



Transactons contain encrypted and digitally signed data along with an index that points to the prior block in the blockchain. Transactions are structured into blocks and recorded in chronological order.

Source: Laura A Linn, Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research

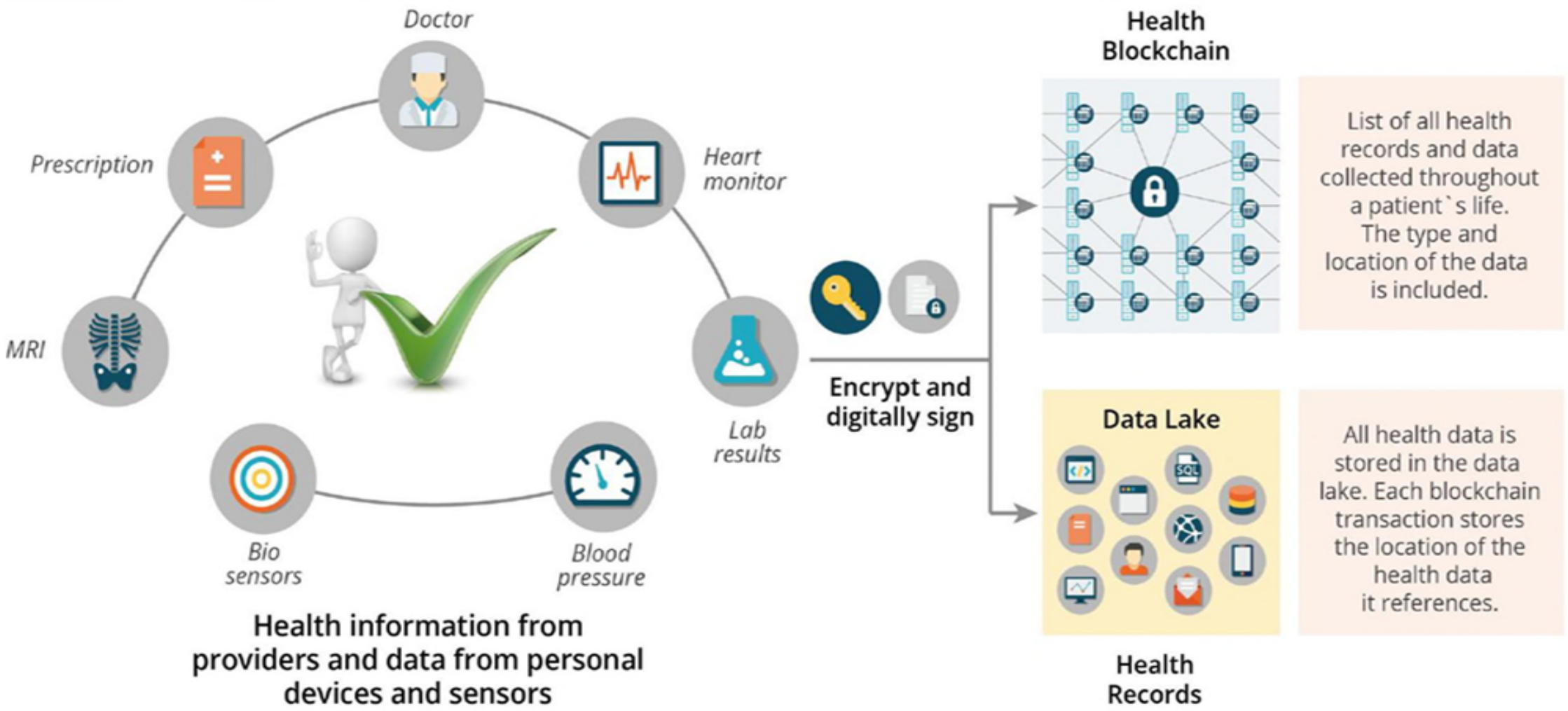
Data Lake

Ingest
Original data of any size and format loaded or streamed into the data lake

Data Lake

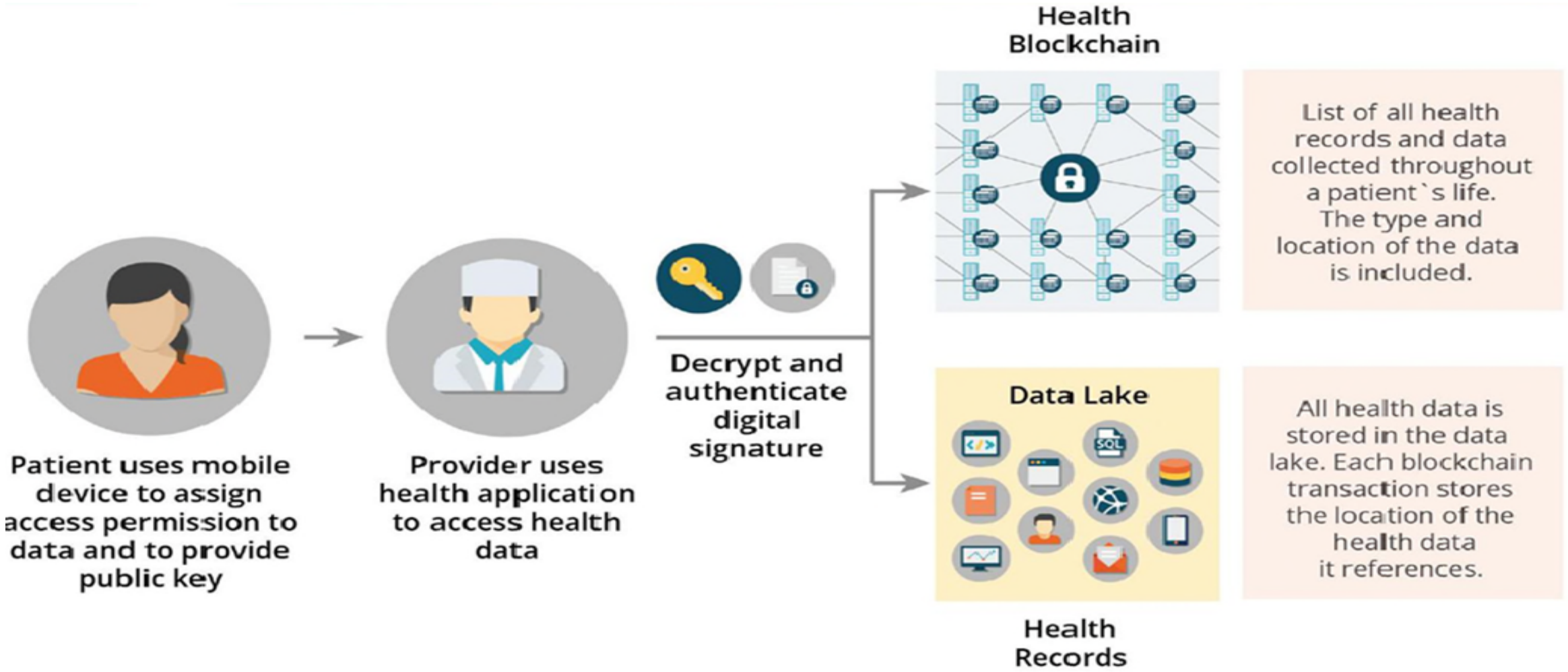
- ✓ Batch queries
- ✓ Interactive queries
- ✓ Real-time analytics
- ✓ Machine Learning

Health Care and Blockchain

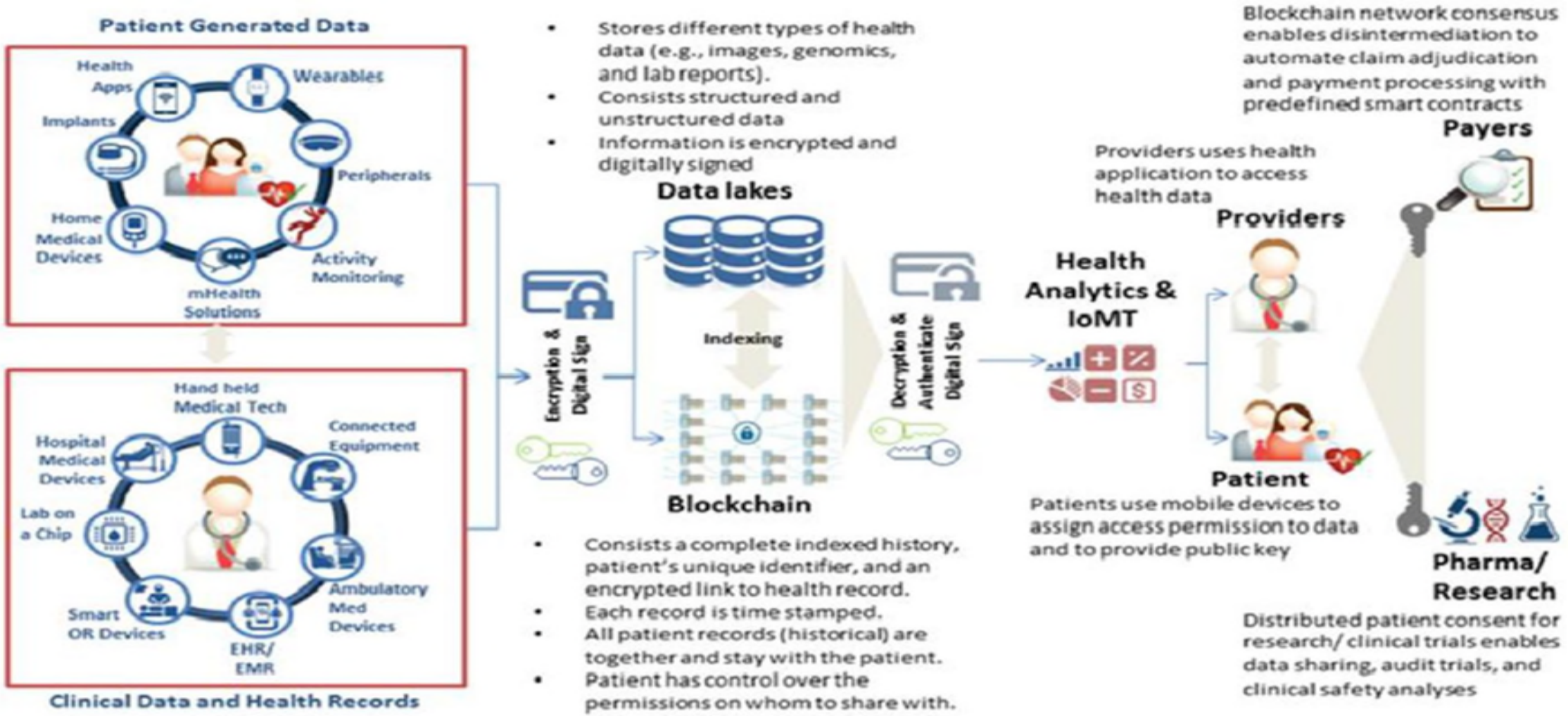


Source: Laura A Linn, Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research

Health Care and Blockchain

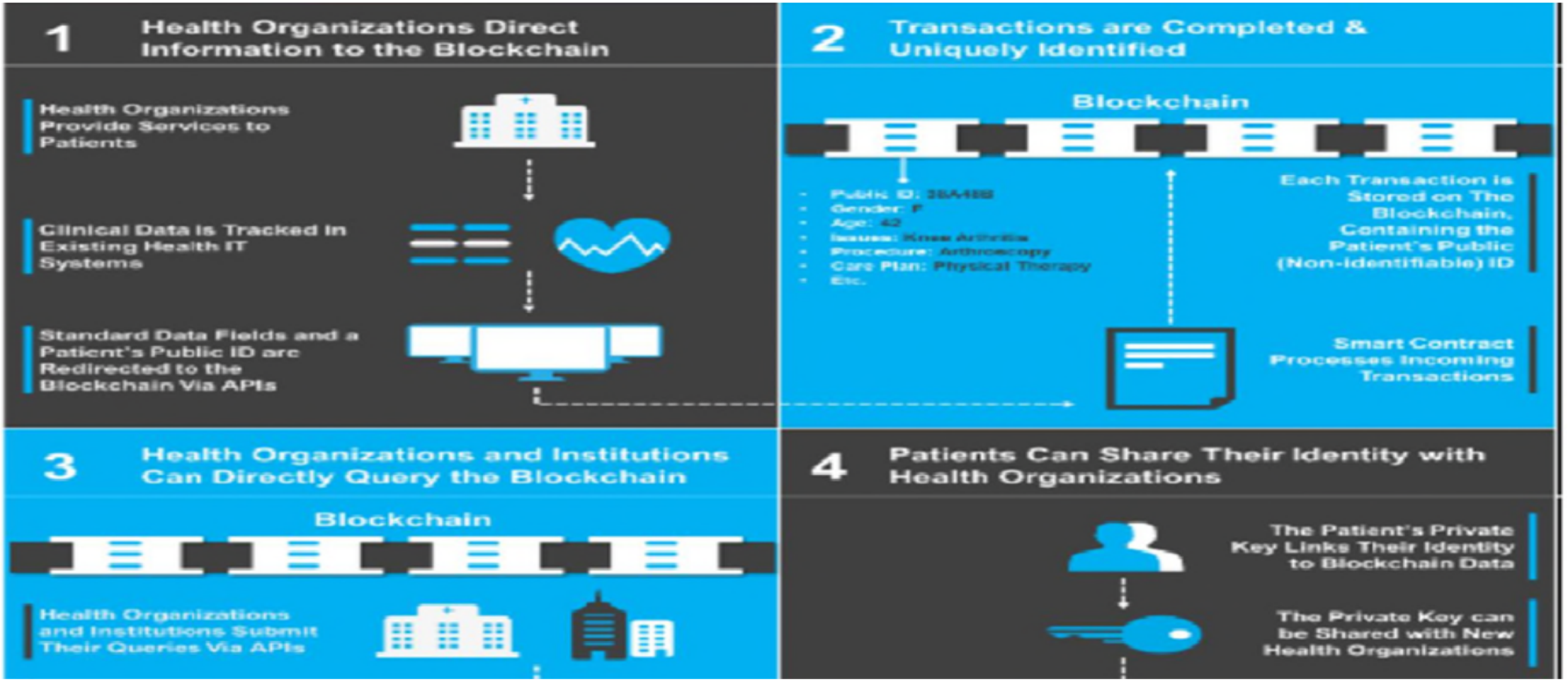


Health Care and Blockchain



Source: Laura A Linn, Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research

Health Care and Blockchain



Source: Deloitte, Blockchain: Opportunities for Health Care (Aug. 2016).

Advantages

- Blockchain technology offers many advantages for health care IT.
- Blockchain is based on opens source software, commodity hardware, and Open API's.
- These components facilitate faster and easier interoperability between systems and can efficiently scale to handle larger volumes of data and more blockchain users.
- The architecture has built-in fault tolerance and disaster recovery, and the data encryption and cryptography technologies are widely used and accepted as industry standards.
- The health blockchain would be developed as open-source software.

Advantages

- Open-source software is peer-reviewed software developed by skillful experts.
- It is reliable and robust under fast changing conditions that cannot be matched by closed, proprietary software.
- Open-source solutions also drive innovations in the applications market.
- Health providers and individuals would benefit from the wide range of application choices and could select options that matched their specific requirements and needs.
- Blockchain technology offers many advantages to medical researchers, health care providers, care givers and individuals.
- Creation of a single storage location for all health data, tracking personalized data in real-time and the security to set data access permissions at a granular level would serve research as well as personalized medicine.

Health Care and Blockchain

- The most efficient and effective approach for advancing interoperability objectives would be to establish a national technology infrastructure for health IT based on open standards.
- Open APIs based on industry best practices are vital and essential to addressing interoperability.
- However, open API's are essential but not sufficient.
- A shared distributed infrastructure that provides a comprehensive view of an individual's health data across a lifetime is an equally essential component of interoperable health IT systems.
- Blockchain technology addresses interoperability challenges, is based on open standards, provides a shared distributed view of health data and will achieve widespread acceptance and deployment throughout all industries.
- Utilization of the proposed health blockchain described in this paper has the potential to engage millions of individuals, health care providers, health care entities and medical researchers to share vast amounts of genetic, diet, lifestyle, environmental and health data with guaranteed security and privacy protection.
- The acquisition, storage and sharing of this data would lay a scientific foundation for the advancement of medical research and precision medicine, help identify and develop new ways to treat and prevent disease and test whether or not mobile devices engage individuals more in their health care for improved health and disease prevention.

Drug Traceability

- Blockchain has the potential to substantially impact the health care industry as a whole and payers, providers and patients with respect to drug traceability, clinical trials and research, and data management.
- Counterfeiting is a major problem for the pharmaceutical industry.
- 10 to 30% of drugs sold in developing countries are counterfeit
- The market exceeds $200 B annually
- China and India are the major manufacturers
- Ingredient and dosages are impacted – which may cause adverse reactions or not provide the expected treatment

Drug Traceability

- Traceability efforts face must connect multiple partners within the supply chain outside traditional transactions (orders, purchase orders, invoices, advance ship notices, etc.) that typically take place between two known trading partners with established electronic connections.

- In track-and-trace environments, a product may make several stops along the way to the end company or customer. To track or trace a product, supply chain partners must either push transaction data from one to another or connect with a trading partner to retrieve transaction data as needed.

- The challenge of track-and-trace solutions is to enable ad hoc connections and provide a means to verify the newly connected partner.

Drug Traceability

- Blockchain provides security in the process
- Manufacturer marks with a unique code# is produced for the drug (contains all relevant information)
- The drug information is stored on the blockchain
- Each time the drug is moved in the process, that information is stored on the blockchain – wholesaler verifies and sends to pharmacist, pharmacist delivers to the patent
- Various studies are occurring through supply chains and with reference to the U.S. Drug Supply Chain Security Act

Clinical Trials

- Mistakes or fraud may occur
- Considerable amounts of data are produced from the trials themselves including safety, efficiency and quality data
- Many people will “touch” this data
- Data collection may not be standardized
- Outcome switching, data dredging and selective publication of results may occur and may also affect protocol development

Clinical Trials

Blockchain can provide authentication and prevent modification:

- Provides proof of existence for and verification of trial data and transparency
- Would include the trial protocol, results, site information, required consents, etc.
- Allows reproducibility and secure data sharing among research communities
- Trial protocol may have a unique signature recorded on the blockchain

- Enables the creation of a system to record and verify clinical trials as specified by the parties conducting the trials and prevents modifications
- Uses an entry from study protocol on clinicaltrials.gov and a text file with pre-specified end points and planned analysis
- Then converted into SHA-256 hash calculator which was then used as a private key for a Bitcoin wallet, followed by a public key to enable transactions

Clinical Trials

- This was followed by an arbitrary bitcoin transaction from a second wallet to the one with the newly generated SHA-256 hash as a private key.
- This transaction recorded the public key on the blockchain, making it easily verifiable over the blockchain.
- Now, anyone with the unformatted text containing a clinical trial protocol may follow the same steps to generate a public key, corresponding to the one that was initially generated and verified over the blockchain by making an arbitrary transaction.
- If the public key in both the cases matches, it not only proves the existence of the document with a time stamp but also verifies that the document has not been changed in any way. In case of any changes, the SHA-256 hash created will be different from the original one, resulting in a different public key.

Patient Data Management

- Managing patient data requires complete access the individual medical records to be shared among various clinicians and other professionals and to and from various locations.
- No standards for collection, storage or disclosure of such information.
- Social networks and physician portals are not always secure.
- Patients do not control their data.

Patient Data Management

- Blockchain can provide a secure structure for:
- Users to share information
- Information can be stored in smart contracts containing permissions and conditions for release
- Patients control access – private keys unlock access or third parties authorized by the patients can do so
- Can pull in other information from wearables and registries
- Companies are building personal health records (PHR) to align all stakeholders through patient engagement platforms and utilizing blockchains to implement

Patient Data Management

- ONC issued an informational blockchain challenge to address the sensitive nature health data and challenges of interoperability, patient record matching and information exchange.
- Critical issues include:
- Creating a trusted environment for determining how multiple providers can view, edit and share patient data while maintaining up-to-date records – that EHRs were not designed to manage.
- Allowing providers to add new records and patients to authorize sharing.
- Blockchain can:
  - Address patient consent for data sharing not addressed by HIEs
  - Provide more tailored consents and update as desired
  - Create a system of “smart contracts” for a rule-based method for access

Patient Data Management

- Store certain data on the blockchain but still allow certain data to be accessed by secure links:
- On blockchain data could include age, gender and other personally identifiable information; be of the size and type to be stored and be immediately viewable
- Off blockchain data could include images and medical notes of any size or format that may have different requirements for the need to view.
- Blockchain could also collect information from web-based and mobile applications or other devices and becomes very important for digital health
- Development and other costs, concern of patients, scalability, storage limits and capacity are obstacles to be addressed

Blockchain for EHR Interoperability and Exchange of Big Data

- Blockchain provides the validation that health care industry needs, and delivers in a way all parties can trust. No single entity is in charge of holding the data, but all participants are responsible for ensuring data integrity and security.

- If no one can change a record without all stakeholders approving the changes, and no unauthorized party can access the health record without the participants giving collaborative permission, the health care industry can avoid two of its most dangerous big data risks at the same time.

- Patient care may benefit from the idea that a readily available verifiable record is instantaneously shared among stakeholders and does not rely on manual data reconciliation prone to human error.

Blockchain for EHR Interoperability and Exchange of Big Data

- Health care organizations may need to limit the number of authorized participants in a single blockchain to a patient, and his or her care team and approved family members.
- This collaborative approach to creating and sharing data would eliminate many of the challenges of HIEs, including the question of how much to trust the middleman.
- While some HIEs have already taken a decentralized approach to their data architecture, the validation piece has been missing. Patients and providers have had to trust that the HIE knows what it's doing and take it on faith that the records moving back and forth between hospitals, specialists, or care facilities are the best possible version of the patient's history.
- When using a blockchain approach to sharing a patient's record, the question of trust is irrelevant since every participant is known and has been approved.
- The implications of blockchains for population health management, patient matching, and care coordination are massive. In addition. Health Care organizations will not compete for, or be unwilling to share, data since they will all have exactly the same information.

Other Uses of Blockchain in Health Care

- Blockchain may also be used for:
- Provider licensing and credentialing
- Payer administration and data exchange for value-based care
- Supply chain management and medication monitoring
- Public health surveillance and population health management
- Revenue cycle management and fraud prevention.

Presenter Biographies

Matt Austin prosecutes complex white-collar crimes for seven years as an Assistant United States Attorney ("AUSA") with the United States Attorney's Office and three years as a state prosecutor with the First Circuit Solicitor's Office. He quickly established himself in the private sector, building a diverse practice representing clients in some of the most high-profile matters in the nation. He routinely provides guidance to elected officials, corporate executives, and ultra-high net worth individuals navigating complex, high-stakes situations including government investigations and indictments, whistleblower complaints, and internal investigations.

Kevin Tran assists financial institutions and technology clients with financial regulatory, securities, and corporate matters. He focuses on the representation of early stage, mid-stage, and publicly traded FinTech companies focused on blockchain technology, digital assets, and cryptocurrencies, including broker-dealers, digital asset and currency trading platforms, digital asset custodians, alternative trading systems, and securities exchanges and swap execution facilities.

Moderator

Richard B. Levin is a partner at Nelson Mullins and is the chair of the FinTech and Regulation Practice and was one of the first lawyers to focus on the regulation of blockchain and digital assets. He is considered a thought leader in the FinTech space. Richard brings his experience as a senior legal and compliance officer on Wall Street and in London to bear in advising clients on corporate, FinTech, securities, and regulatory issues. A problem-solver by nature, he has been advising FinTech clients on legal and regulatory issues since the start of electronic trading in the late 1990s. His practice focuses on helping financial services and technology clients identify and address regulatory issues as they build their businesses. Richard's practice focuses on the representation of early stage and publicly traded companies in the FinTech space, including investment banks, broker-dealers, investment advisers, peer-to-peer lending platforms, digital currency trading platforms, alternative trading systems (ATSs), exchanges, and custodians. He represents these firms before the U.S. Securities and Exchange Commission (SEC), the U.S. Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), the U.S. Department of the Treasury, Office of the Comptroller of the Currency (OCC), state regulators, and Congress. Richard has represented clients before regulators in Australia, Canada, France, Germany, Hong Kong, Ireland, Japan, Singapore, South Korea, and the United Kingdom. His current and past clients include leading national financial institutions, multinational financial services holding companies, leading firms in the FinTech space, and institutions engaging in global investment banking, investment management, securities, and other financial services with institutional clients.

Richard has been identified by Chambers and Partners as one of the leading lawyers in the Blockchain and Cryptocurrencies category since the inception of the category. He has been recognized by Chambers for his knowledge on regulatory matters, great relationships with regulators, for helping clients push the boundaries of the FinTech sector, and for his advice on matters such as broker-dealer licensing and alternative trading systems. Richard is routinely quoted by leading publications including Bloomberg, the New York Times, Reuters, and the Wall Street Journal and is a frequent speaker at conferences around the world on the regulation of FinTech, blockchain, and digital assets.

Contact Details

To learn more about the topics discussed or to contact a speaker, please reach out to:

Richard B. Levin
Chair FinTech and Regulation Practice
Nelson Mullins Riley & Scarborough, LLP
1400 Wewatta Street, Suite 500
Denver, CO 80202
Tel. 303.583.9929
richard.levin@nelsonmullins.com

Kevin Tran
Nelson Mullins Riley & Scarborough, LLP
Partner
1222 Demonbreun Street, Suite 1700
Nashville, TN 37203
Tel. 615.664.5322
Kevin.tran@nelsonmullins.com

Matt Austin
Partner
Nelson Mullins Riley & Scarborough, LLP
Liberty Center
151 Meeting Street, Suite 600
Charleston, SC 2940
Tel. 843.534.4301
matt.austin@nelsonmullins.com

About This Publication

- Nelson Mullins provides this material for informational purposes only.
- The material provided herein is general and is not intended to be legal advice.
- Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues.
- Receipt of this material does not establish an attorney-client relationship.
- Nelson Mullins is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.