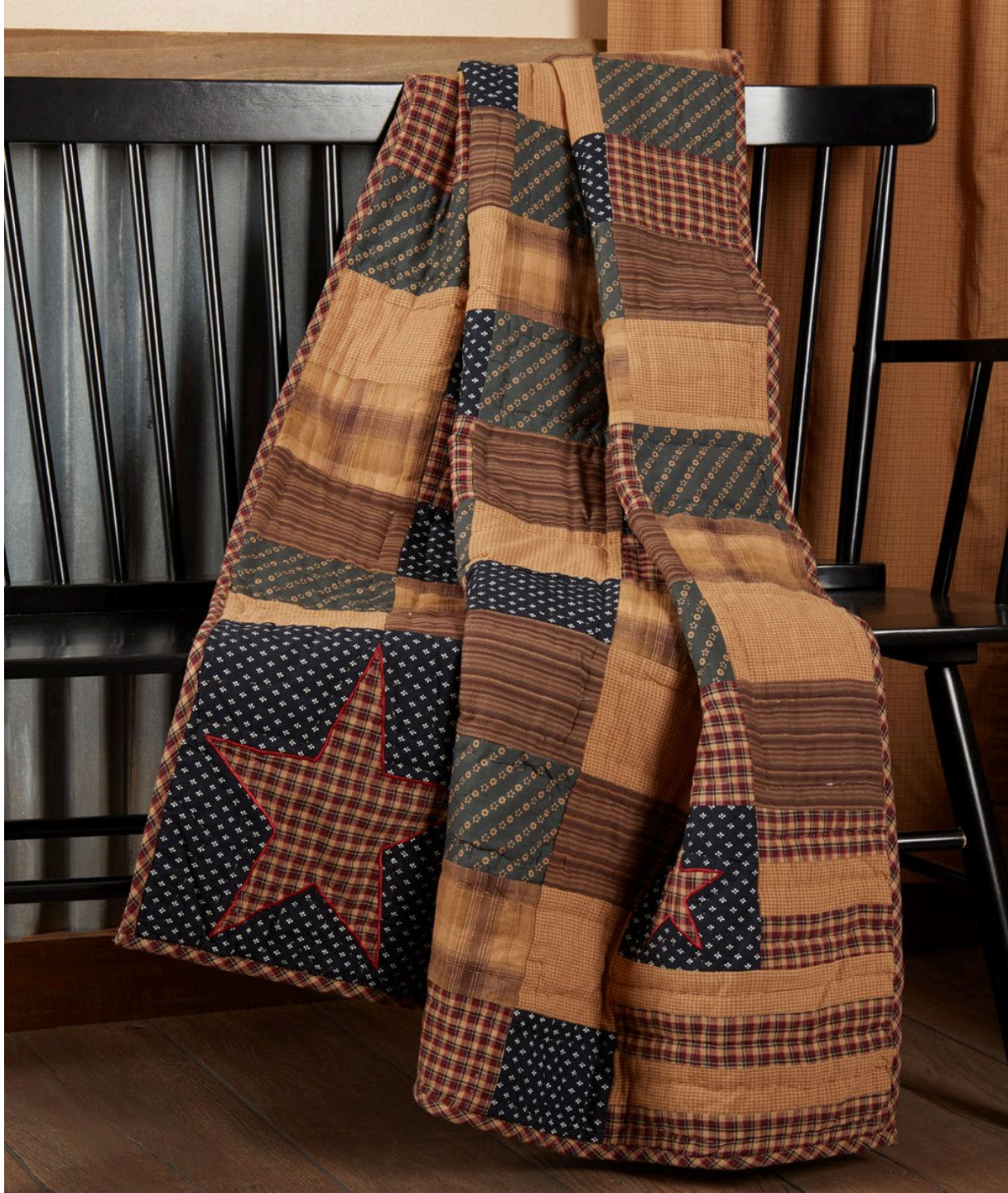
CONTROLLED CONSENT: A BLOCKCHAIN SOLUTION

Protecting Reproductive Health Data in a Post-Dobbs Era

Jacob Williams, Salmon P. Chase College of Law

THE PROBLEM: PATCHWORK LAWS WITHIN THE U.S.

- The current landscape of abortion laws in the U.S. is marked by significant uncertainty, with many states enacting trigger laws that restrict access. Key statistics reveal that a growing percentage of women are using health apps, raising concerns about data privacy amidst regulatory changes.
- The fragmented nature of abortion laws mirrors the current state of data privacy regulation, where individual states create their own rules while a comprehensive national standard remains elusive.



REGULATORY GAPS IN HEALTH DATA PROTECTION

- There exists a significant regulatory gap between HIPAA-protected and unprotected health data, leaving many individuals vulnerable. Recent FTC penalties highlight the risks of weaponizing reproductive health data under restrictive state laws, emphasizing the need for stronger protections.

UNDERSTANDING BLOCKCHAIN TECHNOLOGY

Blockchain technology is a decentralized digital ledger that securely records transactions across multiple computers. Its key features—cryptography, immutability, and decentralization—ensure data integrity and privacy, making it ideal for sensitive health information.

Cryptography: Uses digital keys to verify identity while keeping information private. A public key serves as your visible address, while your private key (kept secret) controls access. This allows secure verification without exposing sensitive details.

Decentralization: Data is stored across multiple computers rather than central servers. No single entity controls the information, and transactions are verified by network consensus instead of intermediaries. This gives users direct control over their data.

Security: Once recorded, data cannot be altered or deleted. Each block contains a unique fingerprint (hash) of the previous block, creating an unbreakable chain. Any tampering changes the hash and alerts the network, ensuring a tamper-proof record.

USER DATA WALLET: A PRIVACY SOLUTION

- A user data wallet functions like a personal bank account for your health information. Just as you can authorize specific transactions from your financial account, users can set permissions for which medical providers and health apps can view specific portions of their data. This allows seamless integration with both clinical care and digital health tools while preventing unwanted disclosures to third parties. Importantly, it still preserves proper channels for legitimate legal investigations with appropriate warrants—balancing individual privacy protections with necessary public safety interests.

CHALLENGES VS. BENEFITS: THE PATH FORWARD

- Implementing blockchain solutions in reproductive health faces challenges such as regulatory compliance, technology adoption, and user education. However, the benefits of enhanced privacy, data security, and user empowerment present a compelling case for its adoption.
- While reproductive health data privacy might not be your personal concern today, tomorrow's legal shifts could suddenly make your own sensitive information vulnerable. The protections we establish now will safeguard all of us when the next privacy crisis emerges—because in our increasingly digital world, it's not a question of if your data will be targeted, but when.

THANK YOU

- Jacob Williams
- WilliamsJ122@mymail.nku.edu
- linkedin.com/in/jawilliams96