SARSON FUNDS

Real. Clear. Crypto.™

DIGITAL ASSET INVESTOR GUIDE TO CRYPTOGRAPHY

PREPARED BY SARSON FUNDS

WWW.SARSONFUNDS.COM

UNDERSTANDING HOW CRYPTOGRAPHY POWERS DIGITAL ASSETS

Understanding the basics of cryptography is important to comprehending the mechanics of digital asset transactions and blockchain security.

For the digital asset investor, advances in cryptography present exciting new blockchain technology investment opportunities.

As advanced cryptography solutions for digital assets begin to emerge, they represent a new frontier of exploration for digital asset investors.

PICTURED: SARSON FUNDS TEAM MEMBERS (LEFT TO RIGHT)
JACOB STELTER, LINDSEY TROSTLE, JAHON JAMALI, JOHN SARSON, BRITTANY KEELS, AND BRYAN PROHM

Sarson Funds is pleased to provide this guide to help investors understand cryptography and discover emergent opportunities in digital asset encryption.

Warm regards,

JOHN R. SARSON
MANAGING PARTNER

JAHON JAMALI
MANAGING PARTNER

VISIT US ONLINE AT WWW.SARSONFUNDS.COM FOR MORE RESOURCES.

All investment products are available to accredited and qualified investors only. No bank guarantees. Not FDIC insured. Past performance does not indicate future performance.

Sarson Funds, LLC is a third party marketing company and does not manage assets or provide investment advice. All investment products advertised by or referred to by Sarson Funds, LLC are property of their respective owners and are offered under Regulation D by their respective issuers. All prospective clients must satisfactorily complete investor eligibility and anti-money laundering disclosures before being referred to any investment sponsor. The official terms and objectives of any strategy mentioned by Sarson Funds can only be conveyed through each fund's specific offering documents, including but not limited to its subscription documents, private placement memorandum, and limited partnership agreement. These documents must be read thoroughly prior to investing. These marketing materials may not reflect any portfolio that Sarson Funds or any investment sponsor managed or currently manage. Any historical returns, expected returns, or probability projections may not reflect actual future performance. If you follow these strategies you may lose money, including all money and assets invested. Sarson Funds is not responsible for errors or omissions.

CRYPTOGRAPHY: A BRIEF HISTORY

'CRYPTOGRAPHY' COME FROM TWO GREEK WORDS: 'KRYPTO' MEANING HIDDEN AND 'GRAPHENE' MEANING WRITING.

Two inherent human needs spurred cryptography: to share information and to communicate selectively. The roots of cryptography are found in ancient Rome and Egypt, with the first known evidence of cryptography being the use of 'hieroglyph,' 4000 years ago.

Scholars moved on to using simple mono-alphabetic substitution ciphers during 500 to 600 BC, which involved replacing alphabets of messages with other alphabets using secret rules. The Romans took this further with their own cryptographic substitutions, known as the Caesar Shift Cipher.

Cryptography saw improved techniques through the 15th century with Vigenere Coding, while the 19th century brought the evolution from ad hoc approaches to encryption to more sophisticated methods of information security.

In the early 20th century, the arrival of devices such as the Enigma rotor machine provided more advanced and efficient means of coding information. During World War II, both cryptography and cryptanalysis became excessively mathematical.

SYMMETRIC ENCRYPTION

Until the 1970s, cryptography had been based on symmetric keys.

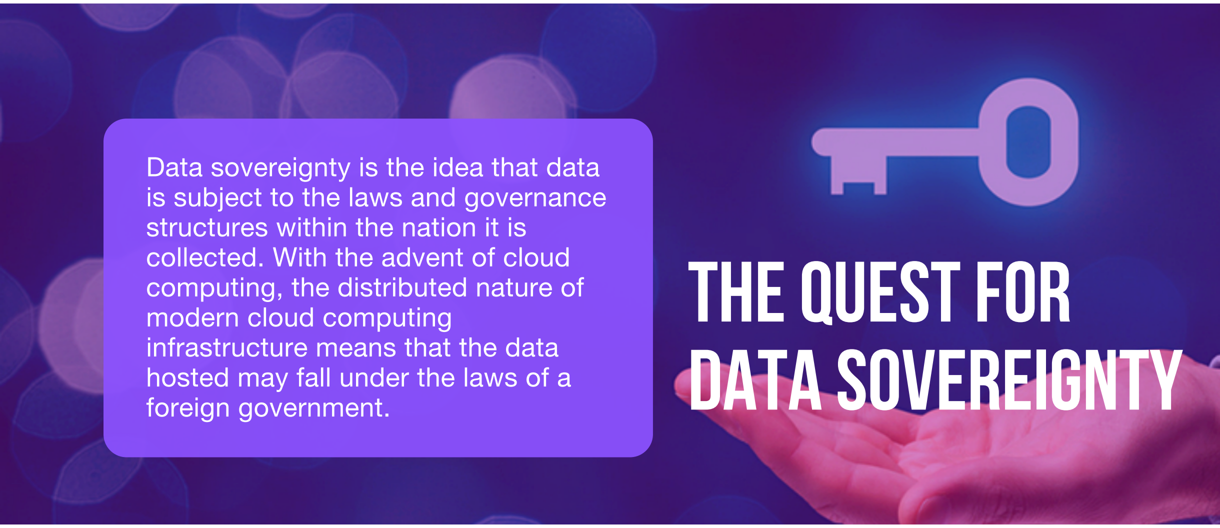
Symmetric encryption utilizes one key to encrypt and decrypt data.

In symmetric encryption, a user's message is encrypted by a password key and sent to another user, who then uses that same password key to decrypt the data into an understandable format.

By encrypting data, it becomes unreadable to anyone without the password key, so the key must be shared in order to decrypt the data and understand the message.

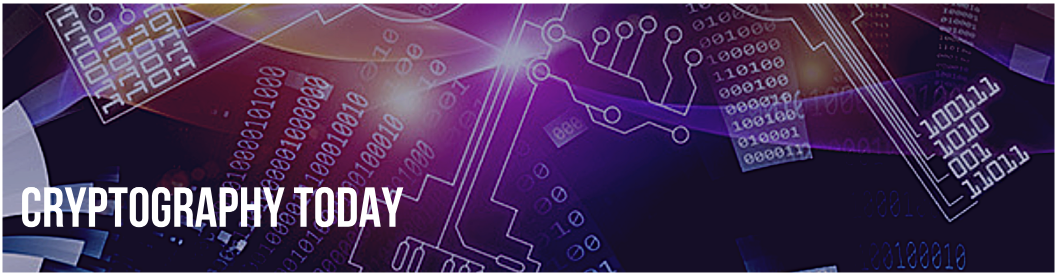
ASYMMETRIC ENCRYPTION

Asymmetric encryption, or public key cryptography, is an enhanced version of symmetric encryption where two password keys are utilized to securitize data for the sole use of the parties meant to use it.



Data sovereignty is the idea that data is subject to the laws and governance structures within the nation it is collected. With the advent of cloud computing, the distributed nature of modern cloud computing infrastructure means that the data hosted may fall under the laws of a foreign government.

THE QUEST FOR DATA SOVEREIGNTY



CRYPTOGRAPHY TODAY

METHODS OF ASYMMETRIC ENCRYPTION EXAMINED

In public key encryption, one key (the public key) is used to encrypt data and another key (the private key) is used to decrypt that data, with each password being the only one that can perform each action. Thus, the public key cannot be used to decrypt the shared data and the private key cannot be used to encrypt that same data. In asymmetric encryption, the public key is made available for public knowledge and the private key is concealed. Asymmetric encryption is used widely in day-to-day communication channels. Popular asymmetric key encryption algorithm includes RSA (Rivest–Shamir–Adleman), DSA (discrete logarithm), and Elliptic curve techniques.

An advanced method to asymmetric encryption is the utilization of prime number factorization and is the approach used in RSA encryption. To utilize this technique, two large prime numbers are found and multiplied together to get a product. Multiplying them together is simple for a computer, but decomposing the product to the two beginning prime factors is computationally infeasible, so far as we know. Of course, since RSA is widely used, it has sparked intense interest in approaches to factorization, so this method may weaken over time.

The discrete logarithm (DSA) approach takes prime number factorization further, and involves finding an integer that solves a logarithmic equation. Elliptic curve encryption utilizes the mathematics of elliptic curves to securitize the private key passwords associated with public key encryption. The elliptic curve approach to encryption is rooted in the assumption that based off of an elliptic model's curvature, guessing the factors of randomly-generated base points, or public key integers, is impractical due to how long it would take to guess the associated private key and decrypt the data. Guessing the private key is impractical because finding it involves solving the discrete logarithm of the randomly-generated base point on the curve, which is challenging because elliptic curve logarithms use practically unsolvable prime number factorization.

CRYPTOGRAPHY IN BLOCKCHAIN

Cryptocurrencies use cryptographic methods to ensure safety and security. Cryptography ensures the safety and security of a transaction by encrypting the data and value of the transaction in the data on the blockchain. Cryptocurrencies use symmetric and asymmetric encryption cryptography. Bitcoin in particular, uses elliptic curve cryptography.

QUANTUM LEAP:
REVISITING ONE-TIME PAD AND HOW QUANTUM COMPUTING WILL DRIVE CRYPTOGRAPHY'S NEXT EVOLUTION

QUANTUM COMPUTING

Unlike ordinary classical computers, quantum computers are constructed on different underlying mechanisms of physics. Because quantum computers rely on different physical mechanisms, they in principle can perform some computations much more quickly than classical computers can. For some encryption algorithms, quantum computing might allow those without the key to entirely sidestep the need to do brute-force search by, for example, enabling a key extraction algorithm that can find the decryption key directly without a blind search.

Public key cryptography algorithms will become breakable as quantum computing becomes more developed.

REVISITING ONE-TIME PAD AND EMERGING ADVANCES IN DIGITAL ASSET CRYPTOCGRAPHY

One-time pad is an encryption technique that cannot be cracked and is the optimum cryptosystem with theoretically perfect secrecy. In this technique, a plaintext is paired with a random secret key. Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. The resulting cyphertext will be impossible to decrypt or break if the following four conditions are met: 1. The key must be truly random, 2. The key must be at least as long as the plaintext, 3. The key must never be reused in whole or in part, 4. The key must be kept completely secret. One-time pads will continue to remain secure even as quantum computing develops.

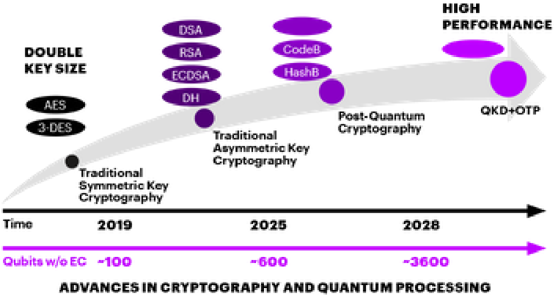
Legacy methods of one-time pad encryption have remained impractical, as they require the use of a one-time, pre-shared key the same size as, or longer than, the message being sent.

Will quantum computing accelerate the market drive for a feasible methodology of one-time pad encryption protocols? We are beginning to witness this today as the continued widespread adoption of digital assets and cryptocurrencies accelerates the demand for cryptographic solutions to a digital asset fueled economy. New investment opportunities in advanced cryptography solutions for digital assets are beginning to emerge and represent a new frontier for the digital asset investor.

CRYPTOGRAPHY
HISTORICAL TIMELINE

400 B.C.	SPARTAN SCYTALE
50 B.C.	CAESER SHIFT CIPHER
1465	VIGNERE CIPHER
1800	JEFFERSON WHEEL CIPHER
1917	VERNAM STREAM CIPHER / ONE TIME PAD
1920	GERMAN ENIGMA
1976	DATA ENCRYPTION STANDARD (DES)
1977	RSA PUBLIC KEY ENCRYPTION
PRESENT	QUANTUM CRYPTOGRAPHY

QUANTUM CRYPTOGRAPHY'S
FUTURE TIMELINE


HIGH PERFORMANCE
DOUBLE KEY SIZE
AES
3-DES
DSA
RSA
ECDSA
DH
CodeB
HashB
Traditional Symmetric Key Cryptography
Traditional Asymmetric Key Cryptography
Post-Quantum Cryptography
QKD+OTP
Time
2019
2025
2028
Qubits w/o EC
~100
~600
~3600
ADVANCES IN CRYPTOGRAPHY AND QUANTUM PROCESSING

(CHART ABOVE, COURTESY: ACCENTURE)

Quantum computing's emergent role in driving new cryptographic solutions has many investors looking for opportunities that provide the security of one-time pad with transactional feasibility.

One-time pads are unconditionally secure in any computation model, if used properly. They are based off of unproven security assumptions and have yet to be broken or show any way of being broken.

Achieving true randomness is essential to incorporating the security of one-time pad level encryption. Emergent solutions of interest to the digital asset investor focus on building upon the concept of truly random irrational numbers, as the square root of a non-perfect square number is irrational, meaning it has no pattern and is truly random.