CRYPTOCURRENCY 101
DIGITAL ASSET INVESTOR GUIDE

PREPARED BY SARSON FUNDS, LLC

WHAT IS CRYPTOCURRENCY?

Throughout the 1990's technology boom, there were many attempts at creating a viable digital currency. Some systems such as PayPal still survive today while most others such as DigiCash, Flooz and Beenz ultimately failed and ceased to exist. There were many different reasons for their failures, such as fraud, financial problems and even frictions between companies' employees and their bosses.

Notably, all of those systems utilized a "Trusted Third Party" approach, meaning that the companies behind the currencies verified and facilitated all transactions. Due to the failures of these companies, the creation of a digital cash system was seen as a lost cause for a long while.

Then, in early 2009, an anonymous programmer or a group of programmers under the alias Satoshi Nakamoto introduced Bitcoin. Bitcoin was the first "cryptocurrency", so named because it didn't rely on a third party but instead used "cryptography" to secure and verify transactions as well as to control the creation of new coins.

Bitcoin introduced the first widespread application of a computer-based consensus network wherein all network participants contributed to the validation of each transaction.

Satoshi described it as a 'peer-to-peer electronic cash system.' It is completely decentralized, meaning there are no servers involved and no central controlling authority.
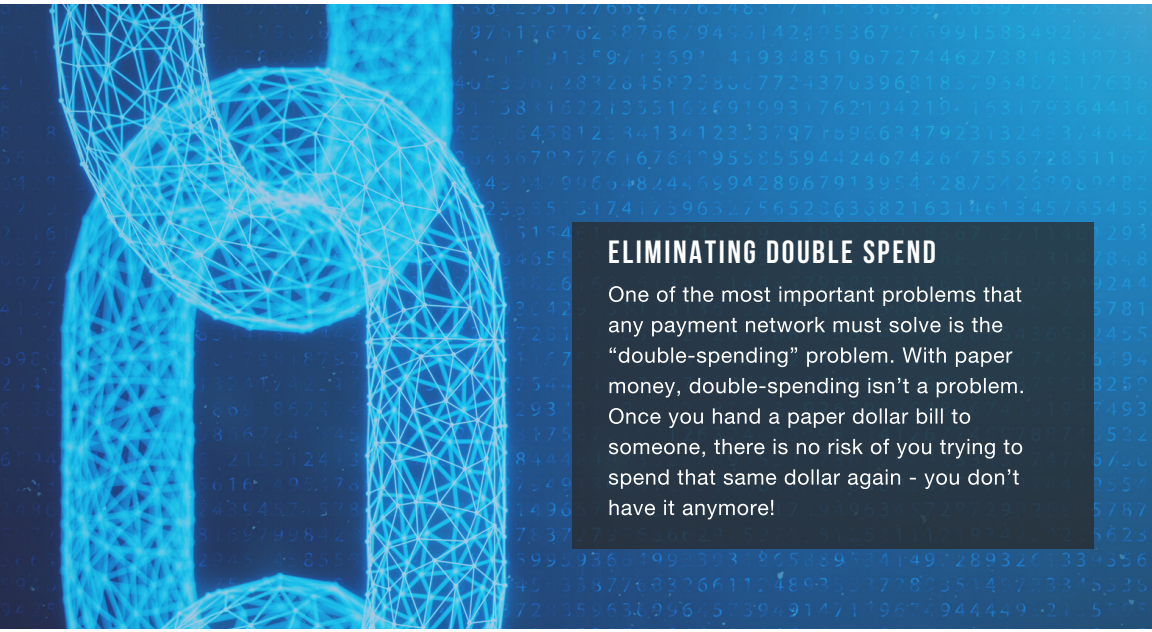
ELIMINATING DOUBLE SPEND

One of the most important problems that any payment network must solve is the "double-spending" problem. With paper money, double-spending isn't a problem. Once you hand a paper dollar bill to someone, there is no risk of you trying to spend that same dollar again - you don't have it anymore!

BLOCKCHAIN TECHNOLOGY

Blockchain technology eliminates digital assets' need for a central controlling authority.

When you send an ACH payment or mail someone a check, a trusted third party – Chase Bank, UBS, Wells Fargo, etc – keeps a record of your balance and reduces your account value by the transaction amount, ensuring that you don't spend the same money twice or spend more than you have.

In the current system, "trusted" banks are in control of your funds and have all your personal details on hand.

In a decentralized network like Bitcoin, all account balances and transactions are recorded via a "Blockchain."

A Blockchain is a public ledger that records all of the transactions that have happened within the network, making the information available to everyone.

Every transaction is a new entry on the Blockchain's public ledger. The entry consists of the sender's and recipient's "public keys" (wallet addresses) and the amount of coins transferred.

The transaction needs to be validated by the sender providing their "private key" (password) and then confirmed by the entire network as to its validity.

Once the transaction is confirmed by the network as valid, the transaction becomes "immutable" (permanent) and that block is added to the blockchain's ledger.

GETTING TO KNOW CRYPTOCURRENCIES
BACKGROUND BEHIND DIGITAL ASSETS

A cryptocurrency is a digital or virtual currency used to store or transfer value.

Cryptocurrencies are so named because they use "cryptography," algorithmically encrypted transmissions, to secure and verify transactions as well as to control the creation of new coins.

Essentially, cryptocurrencies are limited entries in a database that no one can change unless specific conditions are fulfilled.
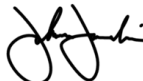
Cryptocurrency and digital assets are here. Many investors have questions about this exciting new asset class.

Sarson Funds is pleased to provide this summary overview of digital assets.

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.

COMMON CRYPTOCURRENCIES

BITCOIN
BTC
THE FIRST AND LARGEST CRYPTOCURRENCY, BITCOIN WAS LAUNCHED IN 2009 AND HAS A CURRENT MARKET CAP OF $80BILLION. BTC'S GLOBAL CONSENSUS NETWORK, WHICH IS POWERED BY ITS USERS, REQUIRES NO CENTRAL AUTHORITY TO OPERATE.

LITECOIN
LTC
THE 'DIGITAL SILVER' COMPARED TO BITCOIN'S 'DIGITAL GOLD.' IT WAS DESIGNED BY RESEARCHERS AT MIT TO BE 4X FASTER AND HAVE 4X TOTAL NUMBER OF COINS AS BITCOIN. IT IS CURRENTLY THE 5TH LARGEST COIN.

ETHEREUM
ETH
A CRYPTOCURRENCY AND A SMART CONTRACT PLATFORM THAT SUPPORTS DECENTRALIZED APPLICATIONS (DAPPS) THROUGH A SCRIPTING LANGUAGE DIFFERENT FROM BITCOIN'S; WITH ROBUST PLATFORM CAPABILITIES AND DEEP POCKETED SUPPORT FROM THE ENTERPRISE ETHEREUM ALLIANCE, ITS $15BILLION + MARKET CAP MAKES IT THE 2ND LARGEST COIN.

POLKADOT
DOT
A STRONG SOLUTION TO THE BLOCKCHAIN TRILEMMA, POLKADOT ENABLES INTEROPERABILITY BETWEEN BLOCKCHAINS TO CREATE A MORE INTERACTIVE AND INCLUSIVE CRYPTO UNIVERSE. THIS TOKEN AND ITS BLOCKCHAIN AIM TO BUILD A COMPLETELY DECENTRALIZED AND PRIVATE WEB GOVERNED BY ITS USERS.

BITCOIN CASH
BCH
A FORK OF BITCOIN THAT IS SUPPORTED BY BITMAIN, THE BIGGEST BITCOIN MINING COMPANY, AND A MANUFACTURER OF ASICS BITCOIN MINING CHIPS. ALL BITCOIN HOLDERS WERE GIVEN BITCOIN CASH FOR FREE DURING THE SPLIT.

EOS
EOS
CONSIDERED A "SECOND-GENERATION" SMART CONTRACT DECENTRALIZED OPERATING SYSTEM BOASTING LOWER FEES, FASTER TRANSACTION TIMES AND USER-FRIENDLY PROGRAMMING LANGUAGES, EOS RAISED $4BILLION IN A YEARLONG "INITIAL COIN OFFERING" WHICH EXCLUDED RESIDENTS FROM THE UNITED STATES IN HOPE OF AVOIDING CONFLICT WITH THE SEC.

NEO
NEO
A SMART CONTRACT PLATFORM THAT HAS MANY OF THE SAME GOALS AS ETHEREUM, BUT DEVELOPED IN CHINA, WHICH COULD POTENTIALLY GIVE IT SOME ADVANTAGES DUE TO IMPROVED RELATIONSHIP WITH CHINESE REGULATORS AND LOCAL BUSINESSES. DUBBED BY SOME AS "CHINESE ETHEREUM."

CARDANO
ADA
CONSIDERED A "SECOND-GENERATION" SMART CONTRACT DECENTRALIZED OPERATING SYSTEM THAT EVOLVED OUT OF A SCIENTIFIC PHILOSOPHY AND A RESEARCH DRIVEN APPROACH. CARDANO USES A DEMOCRATIC GOVERNANCE SYSTEM THAT ALLOWS THE PROJECT TO EVOLVE OVER TIME AND SUSTAINABLY FUND ITSELF.

QUANTUM COMPUTING &
THE FUTURE OF
BLOCKCHAIN TRANSACTIONAL SECURITY

Will quantum computing accelerate a market drive for the rational use of one-time pad encryption protocols? We are beginning to witness this drive today as the widespread adoption of cryptocurrencies and blockchain technology stimulate the demand for uncrackable cryptographic solutions for a digital asset fueled economy. Investment opportunities for advanced digital asset cryptography methods are emerging as a new frontier for cryptocurrency investors.

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 cutting edge cryptographic research 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. Emerging solutions of interest to the digital asset investor will focus on creating practical applications for the one-time pad as the next generation of cryptography.

As this new horizon of investment opportunity develops, we believe Crown Sterling has emerged as the sole provider of one time pad-level encryption solutions. Learn how Crown Sterling is paving the way for the future of true data sovereignty, here: www.crownsterling.io

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