

VERITAS BITCOIN STRATEGIES

D/B/A FAMILY OFFICE BITCOIN

WHITEPAPER

Bitcoin and the Architecture of Wealth Preservation

Interpreting Satoshi Nakamoto's Vision for Family Offices

Eric Runge

Principal, Veritas Bitcoin Strategies, LLC

May 2026

EXECUTIVE SUMMARY

The Argument in Brief

Most analysis of Bitcoin for family offices focuses on its returns, its scarcity, or its place in a diversified portfolio. Each of these is a legitimate analytical angle, and none of them is the most interesting one. This whitepaper argues that the most important property of Bitcoin for multi-generational allocators is something quieter and more structural: the elimination of trusted-third-party dependencies.

In October 2008, an anonymous author writing under the name Satoshi Nakamoto published a nine-page paper proposing an electronic cash system that did not require a financial institution to operate. The proposal's technical contribution was a solution to the double-spend problem in a distributed system without central coordination. The proposal's philosophical contribution was the observation that nearly every monetary instrument in human history has required trust in some third party, and that this requirement is the source of most of the failure modes that monetary systems have experienced. Trust in banks fails when banks fail. Trust in governments fails when governments overreach. Trust in currencies fails when currencies are debased.

For family offices managing wealth across generations, this analysis is not abstract. Every traditional store of value the family office holds is held through a chain of institutional dependencies. Equities are held through broker-dealers and clearing systems. Real estate is recorded by county registrars and protected by jurisdictional law. Cash deposits depend on bank solvency. Even gold, which is itself a bearer instrument, must usually be held through a vault operator and an insurance carrier when held in institutional quantities. Each link in each chain is a point at which the family's claim on the asset can be impaired or denied.

Bitcoin's contribution is not that it removes all such dependencies. As this whitepaper will examine carefully, Bitcoin introduces its own dependencies on cryptography, on network consensus, on custody infrastructure, and on operational discipline. The contribution is that the set of dependencies is structurally different from those of traditional assets, and the differences happen to address several of the failure modes that have historically affected multi-generational wealth most severely.

The body of this whitepaper examines what trust-minimization actually means in technical terms, what kinds of institutional risk it removes, what kinds of new risk it introduces, and how the resulting architecture applies to specific family office use cases. The analysis is neutral. The question for the reader is not whether the trust-minimization framework is sufficient to justify allocation, but whether

the framework correctly identifies a property of Bitcoin that traditional analytical frameworks do not adequately capture.

The question for thoughtful families is not whether Bitcoin belongs in every portfolio. It is whether the unique properties Bitcoin offers — trust minimization, absolute scarcity, and self-sovereign custody — address risks that traditional diversification cannot.

SECTION ONE

What Satoshi Actually Solved

Understanding the trust-minimization argument requires understanding the technical problem Bitcoin was designed to solve. The problem is older than Bitcoin by more than two decades, and the absence of a workable solution had been the principal obstacle to digital cash for that entire period.

The double-spend problem

Money, in any form, must satisfy a basic constraint: each unit must be spendable only once. Physical cash satisfies this constraint trivially because the act of handing over a banknote removes it from the spender's possession. Digital information does not. A digital file can be copied perfectly and used multiple times. In a digital cash system, what prevents the holder of one unit of currency from sending the same unit to two different recipients?

The historical solution has been to interpose a trusted third party. A bank maintains a ledger of who owns what. When a transfer occurs, the bank updates its ledger to reflect the transfer. The constraint that each unit can be spent only once is enforced by the bank's ledger and by the bank's authority to refuse contradictory transactions. This solution works, but it requires that the participants trust the bank to maintain the ledger honestly, to remain operational, and to honor the participants' claims.

Researchers working on digital cash systems prior to 2008 had explored various designs that attempted to minimize the role of the trusted third party. David Chaum's DigiCash used cryptographic blinding to protect the privacy of transactions but still required a central issuer. Wei Dai's b-money proposed a system in which all participants maintained copies of the ledger but did not solve the problem of how participants would agree on which transactions to add. Nick Szabo's bit gold incorporated proof-of-work

to create costly digital scarcity but did not solve the consensus problem either.¹ None of these designs reached production at scale. The double-spend problem in a distributed system without trusted authority was considered analytically open through the mid-2000s.

The Bitcoin contribution

The October 2008 Nakamoto paper proposed a workable solution.² The architecture combined three elements that had each been considered separately in the prior literature but had not previously been integrated: a public ledger replicated across all participants, a proof-of-work consensus mechanism that made it economically irrational to attempt to falsify the ledger, and a longest-chain rule that resolved disagreements about which version of the ledger was authoritative. The integration of these three elements produced a system in which any participant could verify the ledger independently, no participant could unilaterally falsify it, and the cost of attempting to do so would exceed the benefit.

The technical contribution was the workable architecture. The philosophical contribution was the implication: a monetary system could operate without a trusted central authority. The history of money since the development of banking had been the history of accepting institutional trust as the cost of monetary functionality. Bitcoin's proposal was that this cost was no longer necessary.

Bitcoin's contribution was not digital money. Digital money had existed for decades. Bitcoin's contribution was digital money that did not require a trusted intermediary to function.

Why the architecture is structurally different

The architectural significance of Bitcoin lies not in any single one of its features but in the combination. Public ledgers had been studied. Proof-of-work had been explored. Distributed systems had been analyzed extensively. The combination Bitcoin proposed was a system in which the integrity of the ledger rested not on any institution's commitment to maintain it honestly, but on the alignment of economic incentives across thousands of independent participants who would individually find it more profitable to operate honestly than to attempt fraud.

This is a meaningful philosophical move. The Bitcoin system does not eliminate the need for trust altogether. It substitutes one form of trust (trust in a specific institution) with another (trust that

¹The double-spend problem in digital cash systems prior to Bitcoin had been understood since the 1980s. Solutions proposed by David Chaum (DigiCash), Wei Dai (b-money), and Nick Szabo (bit gold) each required some form of trusted authority or central coordination. Bitcoin's contribution was a workable architecture that eliminated the need for any single trusted party.

²Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," October 31, 2008. Published on the cryptography mailing list. The whitepaper introduced the proof-of-work consensus mechanism that solved the double-spend problem in a distributed system without a trusted central authority.

economic incentives will continue to operate as expected and that the cryptographic primitives will continue to hold). Whether this substitution is a net improvement depends on which form of trust is more reliable across long time horizons. The remainder of this whitepaper examines that question.

SECTION TWO

What Trust-Minimization Removes

The Bitcoin architecture eliminates several specific categories of trust dependency that traditional financial assets require. This section examines each category and considers its relevance to multi-generational wealth preservation.

Counterparty dependency

Equities, bonds, and bank deposits all represent claims on institutions. A share of stock is a claim on the issuing corporation and on the broker-dealer maintaining the book-entry record. A bond is a promise by the issuer to pay future cash flows. A bank deposit is a loan to the bank, repayable on demand under normal conditions and subject to legal and operational constraints under abnormal conditions.

Each of these claims can be impaired through institutional failure. The September 2008 collapse of Lehman Brothers vaporized substantial equity and counterparty value in financial markets globally.³ AAA-rated securities issued by major banks and structured finance vehicles became uncollectible in days. Money market funds, considered the safest possible vehicle for liquidity outside bank deposits, experienced broken-buck events. The institutional infrastructure that wealth managers relied on operated under stress conditions for which the standard playbook proved inadequate.

Bitcoin, when held through proper custody architecture, is not a claim on an institution. It is a balance recorded on a distributed ledger, controllable through cryptographic keys. The failure of any specific institution — a custodian, an exchange, a service provider — does not impair the holder's claim to the underlying asset, provided the holder maintains access to the keys. This is structurally different from the counterparty risk profile of traditional securities.

Monetary debasement

The supply of dollars is determined by Federal Reserve policy and federal fiscal decisions. The U.S. monetary aggregate M2 stood at approximately \$700 billion at year-end 1971, immediately following the

³Lehman Brothers Holdings filed for Chapter 11 bankruptcy on September 15, 2008, with reported total assets of approximately \$691 billion. The bankruptcy estate has continued to make recoveries to creditors over more than a decade; ultimate losses to various creditor classes have varied substantially. Characterization of the event as a wealth-destruction episode is supported by the substantial losses to equity holders, junior creditors, and counterparties relying on Lehman's continued operation.

suspension of dollar convertibility to gold. By January 2026, M2 had grown to approximately \$22.4 trillion, an expansion of approximately 32 times.⁴ U.S. population over the same period grew from approximately 207 million to approximately 340 million, an expansion of approximately 1.6 times. The growth in nominal money supply has substantially exceeded the growth in real economic activity for which money is the unit of account.

The Consumer Price Index reflects part of the consequence. The dollar has lost approximately 87 percent of its purchasing power since 1971 by the BLS CPI measure.⁵ The CPI does not capture asset price inflation, which has been substantially larger over the same period: equity indices, residential real estate, and most other traditional store-of-value assets have appreciated in nominal terms by amounts substantially larger than CPI.

Bitcoin's supply is fixed at 21 million units, enforced by network consensus rules.⁶ The issuance schedule is determined in code, not in policy: new Bitcoin enters circulation through a programmatic schedule that halves every four years and asymptotically approaches the cap.⁷ Approximately 19.7 million units have been issued as of early 2026. The remaining issuance occurs over more than a century. The supply property cannot be modified except through coordinated agreement of network participants whose economic interests are aligned in maintaining the cap.

Dollars are not scarce in any structural sense; their supply can be expanded at policy discretion. Bitcoin's supply is structurally fixed. Across long enough time horizons, this difference compounds.

Jurisdictional risk

Wealth held in traditional forms is subject to the legal authority of the jurisdiction in which the assets are located or in which the institutional custodian operates. Equities held in U.S. brokerage accounts are subject to U.S. securities law and U.S. court jurisdiction. Real estate is subject to property tax, eminent

⁴Federal Reserve, M2 money stock data (FRED series M2SL). M2 stood at approximately \$700 billion at year-end 1971 and approximately \$22.4 trillion at January 2026, representing approximately 32x nominal expansion. U.S. population grew from approximately 207 million to approximately 340 million over the same period, representing approximately 1.6x growth.

⁵U.S. Bureau of Labor Statistics, Consumer Price Index for All Urban Consumers (CPI-U). Cumulative dollar purchasing power loss from January 1971 to early 2026 is approximately 87 percent. Source: BLS CPI Inflation Calculator.

⁶Bitcoin protocol specification, Nakamoto (2008) and Bitcoin Core implementation. The 21 million unit supply ceiling is enforced through consensus rules embedded in the reference software and replicated across the global network of validating nodes. Modifying the cap would require coordinated agreement among economically opposed network participants — a coordination problem that has thus far proven intractable.

⁷Bitcoin's issuance schedule halves approximately every 210,000 blocks, or roughly every four years. Initial block subsidy was 50 BTC; the current subsidy following the April 2024 halving is 3.125 BTC. The final fractions of a Bitcoin are expected to be mined around the year 2140.

domain, and zoning authority of the relevant local government. Bank deposits are subject to the freezing authority of the courts and of regulators in the bank's jurisdiction.

History provides examples of jurisdictional authority being applied in ways that affected substantial wealth. Executive Order 6102, issued in 1933, required U.S. persons to surrender gold coin, bullion, and certificates at the prevailing official price; subsequent revaluation of gold to \$35 per ounce represented a 69 percent devaluation of the dollar against gold for those who had complied.⁸ The Argentine corralito of 2001 effectively froze the majority of bank deposits for months. The Cypriot deposit levy of 2013 imposed losses on uninsured deposits at the two largest banks.⁹

Bitcoin held under proper custody architecture is not located in any single jurisdiction. The ledger is replicated globally. Access to the asset depends on possession of cryptographic keys, which can be stored in any jurisdiction or split across multiple jurisdictions. This does not place Bitcoin outside the reach of legal authority; courts can compel the disclosure of keys, and tax authorities can require reporting of Bitcoin holdings. But the asset itself is not seized through the kinds of administrative or court actions that historically have affected wealth held in jurisdictionally concrete forms.

Censorship of value transfer

Financial transactions in traditional systems can be blocked, delayed, or reversed by intermediaries. Banks can refuse to process wires. Payment processors can deny service to specific merchants or individuals. Court orders can freeze the transfer of assets pending resolution of disputes. These powers exist for substantial public-interest reasons, including anti-money-laundering, sanctions enforcement, and consumer protection. They also have been used in ways that affect parties without clear legal due process.

Bitcoin transactions, once initiated by the holder of the keys, are propagated across the global network and confirmed by independent miners. No single party can prevent a properly-signed transaction from being included in the ledger. This property, often described as censorship resistance, is structurally different from the transfer characteristics of traditional financial assets. The implications are not unambiguously positive — the same property that protects legitimate transactions from improper interference also protects illegitimate transactions from proper interference — but the property is real and structurally novel.

⁸Executive Order 6102, issued by President Franklin D. Roosevelt on April 5, 1933, required the surrender of gold coin, gold bullion, and gold certificates by U.S. persons. The official price at surrender was \$20.67 per troy ounce. The Gold Reserve Act of 1934 subsequently revalued gold to \$35 per troy ounce, representing a 69 percent devaluation of the dollar against gold. Holders who surrendered gold prior to revaluation received pre-revaluation pricing.

⁹The Argentine corralito of December 2001 limited bank withdrawals to a small fixed weekly amount and effectively froze the majority of Argentine bank deposits for months. The Cypriot deposit levy of March 2013 initially proposed a tax on all bank deposits as part of an EU/IMF bailout; the final terms imposed losses on deposits above 100,000 euros at the two largest Cypriot banks. Both episodes illustrate the realized risk to depositors in modern banking systems.

SECTION THREE

What Trust-Minimization Does Not Remove

The strongest version of the trust-minimization argument is also the most carefully qualified. Bitcoin does not eliminate trust dependencies altogether; it substitutes one set of dependencies for another. The substitution may be favorable for many multi-generational allocators, but the new dependencies are real and should be evaluated honestly.

Cryptographic dependency

Bitcoin's security rests on the continued mathematical hardness of specific cryptographic primitives, including SHA-256 hashing and elliptic curve signatures over the secp256k1 curve.¹⁰ These primitives are considered secure against all known classical attacks. They are not provably secure; security rests on the practical infeasibility of attacks rather than on mathematical impossibility. A fundamental mathematical breakthrough that compromised these primitives would compromise Bitcoin.

A more practical near-term concern is the development of quantum computers capable of breaking elliptic curve signatures through Shor's algorithm. Sufficiently large quantum computers do not currently exist. Whether they will be built and at what scale is debated. The Bitcoin protocol can be upgraded to post-quantum signature schemes, but such an upgrade has not yet been deployed and would require coordinated network adoption. Family offices planning to hold Bitcoin across multi-decade horizons should consider quantum risk as a real if uncertain factor.

Network consensus dependency

Bitcoin's ledger integrity rests on the continued willingness of independent miners and node operators to maintain the network honestly. The economic incentives for honest operation are substantial and have proven sufficient for more than seventeen years of continuous operation. They are not guaranteed in perpetuity.

Scenarios in which network consensus could fail include a substantial decline in mining incentives below the level required to secure the network economically, coordinated attack by participants controlling a majority of mining capacity, or protocol governance disputes leading to chain splits. None of these has

¹⁰Cryptographic primitives underlying Bitcoin include SHA-256 hashing and ECDSA signatures over the secp256k1 elliptic curve. Both are considered secure against known classical attacks. Sufficiently large quantum computers, if built, could in principle compromise ECDSA. The Bitcoin protocol can be upgraded to post-quantum signature schemes, but such an upgrade has not yet been deployed and would require coordinated network adoption.

occurred at scale, but each is a residual risk that the family office should consider when evaluating multi-decade allocation horizons.

Custody dependency

Although Bitcoin can in principle be held without an intermediary, in practice institutional Bitcoin custody at scale almost always involves dedicated custody infrastructure. Family offices generally engage qualified custodians (Coinbase Custody, Fidelity Digital Assets, BitGo Trust Company, or others) for the operational complexity of secure key management, succession planning, audit support, and integration with traditional reporting systems. This reintroduces a counterparty dependency, although the trust company structure used by major Bitcoin custodians is designed to make the dependency bankruptcy-remote and operationally robust.¹¹

The custody question is a substantial topic in its own right and is treated separately in the firm's parallel whitepaper on Bitcoin custody architectures. The point relevant here is that the trust-minimization property of the Bitcoin protocol does not translate automatically into elimination of operational counterparty risk at the family office level. Realizing the protocol's benefits in operational practice requires deliberate custody architecture choices.

Operational and human-factor dependency

The most common form of loss in institutional Bitcoin holdings, by all available evidence, is not theft or institutional failure but operational error and key loss. Bitcoin held under proper custody architecture is secure against external attack and bankruptcy-remote from custodian failure, but it remains vulnerable to errors by the holder or the custodian: lost keys, incorrectly transmitted transactions, succession failures, social engineering attacks against key holders. These risks have no analog in traditional asset custody at comparable scale and require operational discipline that family offices may not be accustomed to maintaining.

A balanced view

¹¹Bitcoin custody risk takes several forms: total loss of private keys through error or disaster, theft through compromise of custody infrastructure, loss of access through custodian operational failure, and loss through coercion against key holders. These risks differ in kind from traditional securities custody risks and require dedicated operational planning that institutional investors may not be familiar with from other asset classes.

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
C o u n t e r p a r t y / i n s t i t u t i o n a l f a i l u r e	S u b s t a n t i a l d e p e n d e n c y o n m u l t i p l e n	R e d u c e d ; s o m e r e s i d u a l c o s t o d y d e p e n d

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
	t e r m e d i a r i e s	e n c y
M o n e t a r y d e b a s e m e n t	S u b s t a n t i a l f o r f i a t - d	N e g l i g i b l e b y p r o t o c o l

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
	e n o m i n a t e d c l a i m s	d e s i g n
J u r i s d i c t i o n a l / p	S u b s t a n t i a l o r a s s	R e d u c e d ; n o t e l i m i

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
o l i t i c a l a c t i o n	s e t t h e l i n s p e c i f i c j u r i s d i c t i o n s	n a t e d

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
C e n s o r s h i p o f v a l u e t r a n s f e r	S u b s t a n t i a l v i a b l e r e s	M i n i m a l o n c e t r a n s a c t i o n i s p r o p a g a t

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
		e d
C r y p t o g r a p h i c c o m p r o m i s e	L i m i t e d r e s i d u a l r i s k	R e a l i f u n c e r t a i n ; q u a n t u m i s t h e p r

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
		i m a r y c o n c e r n
N e t w o r k c o n s e n s u s f a i l	N o t a p p l i c a b l e	R e s i d u a l b u t h i s t o r i c a

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
u r e		l i q u i t y r e m o t e
O p e r a t i o n a l e r r o r a n d k e y l	L i m i t e d a l l o c a t i o n s ;u n i q u e t o d i c	S u b s t a n t i a l ;u n i q u e t o d i c

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
o s s	c a l e	i t a l b e a r e r a s s e t s
p r i c e v o l a t i l i t y	v a r i e s b y a s s e t c l a	S u b s t a n t i a l ; m u l t

R i s k c a t e g o r y	T r a d i t i o n a l a s s e t s	B i t c o i n
	s s	i p l e 7 0 % + d r a w d o w n s h i s t o r i c a l l y

The strongest argument for Bitcoin is not that it eliminates trust. It is that the specific trust dependencies it introduces happen to be different from, and in

several respects more favorable than, the trust dependencies of the traditional alternatives.

SECTION FOUR

Applications to Multi-Generational Wealth

The trust-minimization framework developed above is not principally an argument about returns. It is an argument about the structural character of the asset. The relevant applications to family office practice are those in which the structural character matters more than the return character.

Portfolio diversification

Bitcoin's historical correlation with traditional asset classes is one component of the portfolio case. During the 2014–2020 period, rolling correlation between Bitcoin and the S&P 500 was generally in the range of 0.0 to 0.2, supporting characterization of Bitcoin as a meaningfully uncorrelated asset. Since the January 2024 SEC approval of spot Bitcoin ETFs, however, rolling correlations have risen to approximately 0.4 to 0.6 depending on measurement window.¹² The shift reflects the integration of Bitcoin into traditional institutional asset allocation flows and broader risk-on / risk-off market dynamics. Bitcoin's historical diversification benefits should not be assumed to persist unchanged into future periods.

That said, a portfolio diversification argument grounded in the trust-minimization framework is structurally different from one grounded in historical correlation. Even if Bitcoin's short-term correlation with equities remains elevated, the asset retains its structural properties: fixed supply, censorship resistance, jurisdictional portability. In scenarios in which the broader monetary or institutional system experiences stress, Bitcoin's properties may diverge from equities even if short-term price correlations have been historically high. The diversification argument from the trust-minimization framework is about tail-scenario behavior, not about ordinary-period correlations.

Tail-risk hedging against monetary disorder

For family offices whose risk frameworks give meaningful weight to scenarios involving currency debasement, sovereign debt crises, or banking system stress, Bitcoin's structural properties offer a tail-risk hedge that traditional diversification does not. Gold is the closest traditional analog, and many family offices hold gold for similar tail-scenario reasons. Bitcoin's structural properties resemble gold's in

¹²Rolling correlation between Bitcoin and the S&P 500 has shifted significantly since 2020. From 2014–2020, the correlation was generally in the range of 0.0–0.2. Since the January 2024 SEC approval of spot Bitcoin ETFs, rolling correlations have risen to a range of approximately 0.4–0.6, depending on the measurement window. Source: aggregated market data; see CoinGecko quarterly correlation reports.

several respects (fixed supply, no counterparty dependency in proper custody) and differ in others (digital portability, programmable inheritance, substantially higher price volatility).

The case for Bitcoin as a tail-risk hedge is not that the tail scenarios will occur, but that the family office's allocation framework should include some exposure to assets whose returns are structurally uncorrelated with the institutional system on which the rest of the portfolio depends. Whether Bitcoin or gold or some combination best serves this purpose is a family-specific question.

Generational wealth transfer

Traditional estate planning involves a series of institutional intermediaries: probate courts, executors, attorneys, transfer agents, title companies, and tax authorities. The process typically extends six to twenty-four months for substantial estates and involves federal estate taxes that can reach forty percent above applicable exemptions. International family situations add further complexity through cross-border legal and tax coordination.

Bitcoin permits a substantively different inheritance architecture. Properly structured multi-signature wallets can transfer control through cryptographic procedures rather than through institutional probate. Multi-signature schemes can designate key holders in different jurisdictions, can require multiple parties to coordinate access, and can implement automated time-locked release mechanisms. The result is inheritance that bypasses much of the institutional friction of traditional estate transfer.

The qualifications are substantial. Bitcoin inheritance planning requires specialized legal and tax counsel; the absence of probate does not eliminate tax liability; key management failures can result in permanent loss of the asset; and family education about access procedures is essential. The inheritance case for Bitcoin rests not on the absence of complexity but on the substitution of one form of complexity (cryptographic and operational) for another (institutional and legal), with the substitution being favorable for some families and unfavorable for others depending on circumstances.

Treasury reserve function

Family offices commonly hold five to fifteen percent of assets in cash or cash-equivalent positions for liquidity, opportunistic deployment, and crisis response. The yield on these positions varies with interest-rate conditions but in real terms has been negative for much of the post-2008 era. The function of the cash reserve is optionality rather than return; the cost of holding it is the foregone return on alternative deployments.

Bitcoin as a partial substitute for cash treasury reserve introduces several considerations. On the favorable side: Bitcoin's supply property means the position is not subject to the monetary debasement

that affects cash reserves; the asset is liquid in major institutional markets around the clock; transferable internationally without correspondent banking dependency. On the unfavorable side: Bitcoin's price volatility means short-term liquidity has substantial mark-to-market risk; the asset is not suitable for funds expected to be needed within shorter time horizons; tax treatment of dispositions adds complexity.

Family offices considering Bitcoin in this role typically hold modest percentages (one to three percent of total assets, or proportionally larger fractions of the broader cash reserve) and treat the position as a long-horizon component of the reserve rather than as a near-term liquidity source.

Structured downside protection approaches

Bitcoin's volatility imposes practical constraints on its incorporation into many family office portfolios. Investment policy statements may restrict assets with multi-year drawdown potential exceeding specified thresholds. Trustees and boards may impose risk-management constraints incompatible with unhedged Bitcoin exposure. Multi-generational decision-making dynamics may make it difficult to maintain conviction through the seventy to eighty percent drawdowns that the asset has historically experienced.

Structured downside protection approaches address the tension between long-term Bitcoin exposure and short-term volatility constraints. Such approaches combine direct or indirect Bitcoin exposure with derivative or structured-product overlays designed to cap maximum drawdown at levels lower than unhedged exposure. The general category includes options-based hedging, structured notes, defined-outcome ETFs, and proprietary variations. Each approach trades reduced downside volatility for reduced upside capture relative to unhedged exposure.

Whether a structured approach is appropriate depends on the family office's specific constraints. For families with long horizons, high risk tolerance, and the operational discipline to hold through full cycles, unhedged exposure has historically produced superior cumulative returns. For families with binding volatility constraints, generational governance considerations, or psychological constraints around drawdown experience, structured approaches may convert what would otherwise be a non-allocable position into one that meets the family's actual constraints. Implementation requires specialized analysis of the specific structure proposed, including its cost, its tax treatment, its counterparty risk, and the specific shape of the upside / downside trade-off.

SECTION FIVE

Risks Honestly Stated

The trust-minimization argument is incomplete without a careful statement of the risks Bitcoin introduces. Family offices considering allocation should evaluate the full risk profile, not merely the risks the asset reduces.

Price volatility. Bitcoin has experienced drawdowns exceeding seventy percent on multiple occasions, including 2014–2015, 2018, and 2022.¹³ Multi-year periods of substantial unrealized losses should be considered an expected feature of the asset class rather than an aberration. Future drawdowns may be larger or smaller than historical drawdowns; the historical pattern is not predictive.

Regulatory uncertainty. The legal and regulatory treatment of Bitcoin continues to evolve in the United States and internationally. Specific elements that are likely to change include tax treatment, accounting standards, custody requirements for institutional holders, and the interaction of digital asset rules with existing securities and commodities frameworks. Adverse regulatory developments could materially affect Bitcoin's value, usability, or accessibility.

Custody complexity. Bitcoin custody requires operational discipline that family offices may not be familiar with from other asset classes. Loss of private keys results in permanent and irreversible loss of the asset. Theft through hacking, phishing, or physical coercion are real and have occurred at substantial scale across the industry. Mitigation requires deliberate custody architecture decisions, professional support, and ongoing operational vigilance.

Tax complexity. Bitcoin transactions create taxable events under most U.S. tax positions, including the disposition of Bitcoin for other assets, the use of Bitcoin to acquire goods or services, and certain operational transfers. The tax treatment is more complex than for traditional securities, particularly for active management strategies that involve frequent rebalancing. Family offices considering Bitcoin allocation should engage qualified tax counsel familiar with digital asset taxation before implementation.

Technology and protocol risk. Although the Bitcoin protocol has operated continuously for more than seventeen years without successful attack on the protocol itself, residual technology risks exist. These include the cryptographic and consensus risks discussed in Section Three, the risk of protocol bugs, the risk of chain splits resulting from governance disagreements, and the risk of network conditions making transactions impractical at scale.

Liquidity risk. Bitcoin markets are liquid at moderate institutional scale during normal conditions but can experience substantial slippage on large transactions during stressed conditions. Family offices

¹³Bitcoin's historical drawdowns have exceeded 70 percent on multiple occasions, including 2014–2015, 2018, and 2022. Multi-year periods of substantial unrealized losses should be considered an expected feature of the asset rather than an aberration. Past drawdown patterns are not predictive of future drawdowns; future drawdowns could be larger or smaller in magnitude and duration.

considering large positions should evaluate market microstructure and execution capability as part of the allocation framework, not as an afterthought.

Operational and human-factor risk. As noted in Section Three, the largest source of realized losses in institutional Bitcoin holdings has historically been operational error and human-factor compromise rather than external attack or institutional failure. This risk profile is genuinely different from the risk profile of traditional asset classes at comparable scale and requires operational structures that may be unfamiliar.

SECTION SIX

The Question for the Family Office

The trust-minimization framework does not produce a recommended allocation. It produces a question. The question is whether the structural property of trust-minimization, properly understood and properly qualified, addresses risks in the family's broader portfolio that traditional diversification does not address.

For some families, the answer will be no. Traditional diversification across equities, fixed income, real estate, private equity, and alternative investments may be judged adequate to the family's actual risk profile. The structural property of trust-minimization may be judged either irrelevant to the family's actual concerns or insufficient to justify the volatility and operational complexity that Bitcoin introduces. A zero allocation can be a defensible conclusion of this analysis.

For other families, the answer will be yes, at some modest fraction of the portfolio. A one to three percent allocation positions the family to benefit from the structural properties of the asset without exposing the broader portfolio to Bitcoin's volatility in destabilizing proportions. The position serves principally as a tail-scenario hedge and as exposure to the structural properties rather than as a return-seeking allocation.

For a smaller group of families, the answer will be a larger allocation. Families with longer horizons, higher absolute risk tolerance, or more substantial concerns about the integrity of institutional infrastructure may conclude that the trust-minimization framework justifies five to fifteen percent or more. Such allocations require both substantial conviction and substantial operational sophistication; they should not be approached without deliberate framework, governance, and custody architecture.

The artifact this whitepaper hopes to produce is not a recommended allocation. It is a documented framework through which the family office can reach its own allocation conclusion. That framework should articulate the family's view on the structural properties of the asset, the operational risks of

holding it, the appropriate position size given the family's broader portfolio and constraints, and the conditions under which the allocation would be revised. With such a framework in place, the family office can hold its position through cycles, defend the position to successors and trustees, and revise the position deliberately as circumstances change.

Trust-minimization is not a property that automatically benefits every portfolio. It is a property that addresses a specific category of structural risk. The family office's analytical task is to determine whether that category of risk is material to its own circumstances.

CONCLUSION

Reading Satoshi Carefully

The 2008 Nakamoto paper is nine pages long. Most discussion of Bitcoin in the seventeen years since has focused on the asset class it created, the prices it has reached, and the institutional adoption it has attracted. Less discussion has focused on the underlying analytical claim: that monetary systems have historically required institutional trust as a structural feature, and that this requirement is the source of failure modes that affect wealth most severely across long time horizons.

For family offices managing capital across generations, that analytical claim is the part of Bitcoin worth taking seriously. The price action will continue. The institutional adoption will continue. Neither is the principal reason to take Bitcoin seriously as a multi-generational allocation. The principal reason is that the structural property Satoshi identified — the elimination of certain forms of institutional trust dependency — may, for some families and some portfolios, address risks that the traditional framework does not address.

The question is not whether trust-minimization is the right framework for evaluating Bitcoin. It is whether the framework correctly identifies a property of Bitcoin that other frameworks miss. If it does, the implications for multi-generational portfolio construction are substantial. If it does not, the framework should be discarded. Family offices working through this question carefully will reach different conclusions. None of those conclusions is right or wrong in advance. The work that produces the conclusion is the artifact that matters.

DISCLOSURES

Important Disclosures

Educational purpose. This whitepaper is provided for educational and informational purposes only. It does not constitute investment advice, a recommendation to buy or sell any security, an offer of investment advisory services, or the provision of any legal, tax, or accounting advice. Nothing in this whitepaper should be construed as a solicitation to engage Veritas Bitcoin Strategies, LLC or Eric Runge for advisory services. Allocation decisions should be made in consultation with qualified legal, tax, and investment advisers familiar with the reader's specific situation.

Investment risk. Bitcoin and Bitcoin-related investments involve substantial risk, including the potential loss of principal. Bitcoin is highly volatile, with historical drawdowns exceeding seventy percent. Past performance is not indicative of future results. There is no guarantee that any allocation strategy described or referenced in this whitepaper will achieve its objectives or that any investment will be profitable. Bitcoin is not insured by the Federal Deposit Insurance Corporation, the Securities Investor Protection Corporation, or any governmental agency. Bitcoin is not appropriate for funds needed within short time horizons.

Statistics and data points. Statistics, performance figures, and other data points cited in this whitepaper are drawn from publicly available sources as identified in the footnotes. While Veritas Bitcoin Strategies has taken reasonable care to ensure the accuracy of data cited, readers should verify any specific data point before relying on it for investment decisions. The forward-looking analysis and structural arguments presented in this whitepaper reflect the firm's views as of the date of publication and are subject to change.

Forward-looking statements. Statements about future regulatory developments, monetary policy, institutional adoption, asset performance, or protocol behavior reflect the author's analysis as of the date of publication and may prove incorrect. Forward-looking statements involve inherent uncertainty and should not be relied on as predictions. Tax treatment of Bitcoin transactions may change through legislation or administrative action.

Structured downside protection approaches. The discussion of structured downside protection approaches in Section Four describes a general category of strategies and does not endorse, recommend, or describe any specific product, vendor, or implementation. Family offices considering such approaches should engage qualified advisers to evaluate specific structures against their own circumstances. The general category includes products and approaches with varying costs, complexities, counterparty risks, and tax characteristics.

No specific allocation recommendation. The allocation ranges discussed in Section Six are descriptive of approaches that some family offices have adopted and are not recommendations to the reader. Appropriate allocation depends on family-specific circumstances that this whitepaper does not address

and cannot address generically. Readers should not interpret the allocation ranges as suitable for their own circumstances without independent analysis.

Regulatory disclosure. Family Office Bitcoin, a registered DBA of Veritas Bitcoin Strategies, LLC, is a Registered Investment Adviser in the state of Oregon. Registration does not imply a certain level of skill or training. Form ADV Part 2A and Part 2B are available upon request and through the Investment Adviser Public Disclosure database at adviserinfo.sec.gov by searching CRD #306768.

Conflicts of interest. Veritas Bitcoin Strategies and its principal may hold Bitcoin positions for the firm's own account or in client accounts. Specific conflicts of interest are disclosed in Form ADV Part 2A. The firm uses specific service providers (custodians, executing brokers, and others) in its operations; material business relationships are disclosed in Form ADV and in firm marketing materials addressing the specific services involved. This whitepaper does not recommend specific service providers.