1. Appendix A

Adi Shamir makes 15 predictions for the next 15 years in his anniversary keynote "Financial Cryptography: Past, Present, and Future" at Financial Cryptography 2016: Its origins lie in a mailing list ran by Robert Hettinga who started the Digital Commerce Society of Boston with Ray Hirschfeld, Vince Cate and others. Negative distrust has been overwhelming in the literature: For examples: "Cyber-security is terrible and will get worse. The Internet of Things will be a security disaster. Cyber warfare will be the norm rather than the exception in conflicts. RC4 and SHA-1 will be phased out while AES and SHA-2/3 will remain secure (he expects a SHA-1 collision within the year). Improved factoring and DL algorithms will be found requiring key sizes beyond 2048 (he feels it will not be a fully polynomial algorithm; 4096 should be OK). Elliptic curves will fall out of favor (there's a very strange current situation with the NSA moving away from it with no explanation). Research will still pour into quantum crypto and quantum computing, as the physics community is geared up to accept large amounts of government money. But there will be no full-size quantum computers capable of factoring RSA keys. No-one will use quantum crypto. Governments will not tolerate anonymity. Most people will not demand or expect real privacy; that war is already lost. Tools to fight cybercrime and attacks will further diminish privacy. Bitcoin will fade away but leave a legacy. Blockchain will be hyped, but succeed only in limited circumstances. An endless stream of new payment mechanisms will be presented at future Financial Crypto conferences."

2. Appendix B

Francis Crick and Christof Koch have compared the Claustrum to the conductor of an orchestra, referring to its regulatory role in consciousness and cognition. Claustrum which is a thin, irregular sheet of neurons that is attached to the underside of the neocortex in the center of the brain. It is suspected to be present in the brains of all mammals. The Claustrum in the human brain is a fraction of a millimetre to a few millimetres deep and is a vertical curved sheet of subcortical region. AI can adjust and make decisions based on processing high volumes of data. For example, Apple's Siri. Siri learns your schedule, habits and likes/dislikes by merely tracking data of individual decisions. When patterns are recognized, Siri can make decisions about recommendations and options. AI can be used in all sorts of applications, from B2B to B2C, and in the process, make things faster and easier for the end user. The Boltzmann Machine might take a week by Terry Sejnowski and Geoffrey Hinton of MIT PDP group.

3. Appendix C

The term "hash" offers a natural analogy with its non-technical meaning to "chop" or "make a mess" out of something. Applications from BC Split-Key Vanity Mining Bitcoin addresses are hashes of public keys from ECDSA key pairs, which have homomorphic properties for addition and multiplication.For example, Alice generates a private key (a) and public key (A) pair, and publicly posts A. Bob generates a key pair (b, B) such that hash (A + B) results in a desired vanity address. He sells b and B to Alice. A, B, and b are publicly known, so one can verify that the address = hash (A + B) is desired. Alice computes the combined private key (a + b) and uses it as the private key for the public key (A + B). Similarly, instead of addition, they could have used multiplication.

The configuration and operation of an optical Mach-Zehnder interferometer and its actual realization with electrons. (a) Schematics of an optical Mach-Zehnder interferometer. D1 and D2 are detectors, BS1 and BS2 are beam splitters, and M1 and M2 are mirrors. With 0(π) phase difference between the two paths, D1 measures maximum (zero) signal and D2 zero (maximum) signal. The sum of the signals in both detectors is constant and equals to the input signal. (b) Schematics of the electronic Mach-Zehnder interferometer and the measurement system. Edge states are formed in a high perpendicular magnetic field. The incoming edge state from S is split by QPC1 (quantum point contact) to two paths, of which one moves along the inner edge and the other along the outer edge of the device. The two paths meet again at QPC2, interfere, and result in two complementary currents in D1 and in D2. By changing the contours of the outer edge state and thus the enclosed area between the two paths, the modulation gates (MG) tune the phase difference between the two paths via the Aharonov-Bohm effect. A high signal-to-noise-ratio measurement of the current in D1 is performed at 1.4MHz with a cold LC resonant circuit as a band pass filter followed by a cold, low noise, preamplifier. (c) SEM picture of the device. A centrally located small Ohmic contact (3 × 3μm2), serving as D2, is connected to the outside circuit by a long metallic air-bridge. Two smaller metallic air-bridges bring the voltage to the inner gates of QPC1 and QPC2 - both serve as beam splitters for edge states. The five metallic gates (at the lower part of the figure) are modulation gates (MG).

A country's productive structure and competitiveness are harbingers of growth. Growth is a dynamic process based on capabilities that are difficult to define and measure across countries. This paper uses a global measure of fitness (or complexity-weighted diversity of production) as a method to explore a country's relative growth potential. The analysis finds that there are two types of growth, predictable or laminar, and unpredictable. This classification is used to create a selection mechanism (the Selective Predictability Scheme), defining future growth trajectories for similar countries, and compares projected long-term, five-year forecasts with traditional methods used by the International Monetary Fund. The analysis finds that production structure is a good long-term predictor of growth, with prediction performance falling off for countries not yet in the laminar classification.