Democracy Enhancing Technologies

Jeremy Clark

A Thesis in
The Concordia Institute for Information Systems Engineering (CIISE)

Presented in Partial Fulfillment of the Requirements
For the Degree of
Doctor of Philosophy
(Information and Systems Engineering)
at
Concordia University
Montréal, Québec, Canada Test

September 2023

Concordia University
School of Graduate Studies

This is to certify that the thesis prepared

By: **Jeremy Clark**

Entitled: **Title**

and submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy (Information and Systems Engineering)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Chair
Walter Lucia

_____ External Examiner
Kaiwen Zhang (ETS)

_____ Examiner
Amr Youssef

_____ Examiner
M. Mannan

_____ Examiner
Carol Fung

_____ Supervisor
Jeremy Clark

Approved by _____
Zachary Patterson, Graduate Program Director (CIISE)

01 Sept 2023 _____
Mourad Debbabi, Dean (GCS)

Abstract

Name: **Jeremy Clark**

Title: **Democracy Enhancing Technologies**

Hello. No more than 250 words.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Diam donec adipiscing tristique risus nec feugiat in fermentum posuere. Et netus et malesuada fames ac turpis. Nullam non nisi est sit. Felis eget velit aliquet sagittis id. Mauris commodo quis imperdiet massa tincidunt. Tellus molestie nunc non blandit massa enim nec. Facilisis mauris sit amet massa. Et molestie ac feugiat sed. Metus vulputate eu scelerisque felis imperdiet proin.

Acknowledgments

Hello.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Diam donec adipiscing tristique risus nec feugiat in fermentum posuere. Et netus et malesuada fames ac turpis. Nullam non nisi est sit. Felis eget velit aliquet sagittis id. Mauris commodo quis imperdiet massa tincidunt. Tellus molestie nunc non blandit massa enim nec. Facilisis mauris sit amet massa. Et molestie ac feugiat sed. Metus vulputate eu scelerisque felis imperdiet proin.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Hello.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Diam donec adipiscing tristique risus nec feugiat in fermentum posuere. Et netus et malesuada fames ac turpis. Nullam non nisi est sit. Felis eget velit aliquet sagittis id. Mauris commodo quis imperdiet massa tincidunt. Tellus molestie nunc non blandit massa enim nec. Facilisis mauris sit amet massa. Et molestie ac feugiat sed. Metus vulputate eu scelerisque felis imperdiet proin.

Velit laoreet id donec ultrices tincidunt arcu non. Varius vel pharetra vel turpis nunc. Quis enim lobortis scelerisque fermentum dui faucibus in ornare quam. Lacus viverra vitae congue eu consequat ac felis donec. Consectetur adipiscing elit duis tristique sollicitudin nibh. Aliquam malesuada bibendum arcu vitae elementum curabitur vitae nunc. Sit amet venenatis urna cursus. Mi quis hendrerit dolor magna

eget est lorem. Et ligula ullamcorper malesuada proin libero nunc consequat interdum varius. Id nibh tortor id aliquet lectus proin. Proin nibh nisl condimentum id venenatis a condimentum vitae sapien. Viverra aliquet eget sit amet tellus cras adipiscing. Bibendum ut tristique et egestas quis ipsum suspendisse ultrices gravida.

Mollis aliquam ut porttitor leo a. Nibh mauris cursus mattis molestie a iaculis at. Ultricies leo integer malesuada nunc vel. Feugiat nibh sed pulvinar proin gravida hendrerit lectus a. Eu facilisis sed odio morbi. Gravida arcu ac tortor dignissim. Nisl pretium fusce id velit ut tortor pretium viverra. Felis bibendum ut tristique et egestas. Turpis egestas pretium aenean pharetra magna ac placerat vestibulum lectus. Arcu non sodales neque sodales ut etiam sit amet nisl. Vulputate enim nulla aliquet porttitor lacus luctus accumsan tortor. Sed risus pretium quam vulputate dignissim suspendisse. Malesuada fames ac turpis egestas maecenas pharetra convallis posuere morbi. Aliquet lectus proin nibh nisl condimentum. Nibh sed pulvinar proin gravida. Quis vel eros donec ac odio tempor orci. Dignissim convallis aenean et tortor. Ac tincidunt vitae semper quis lectus nulla at volutpat. Vulputate odio ut enim blandit.

Tellus at urna condimentum mattis pellentesque id nibh tortor. Convallis posuere morbi leo urna molestie. Quis commodo odio aenean sed adipiscing diam donec. Iaculis eu non diam phasellus vestibulum. Tempus urna et pharetra pharetra massa massa ultricies mi. Faucibus turpis in eu mi bibendum neque egestas. Molestie ac feugiat sed lectus vestibulum mattis. Est ullamcorper eget nulla facilisi. In nibh mauris cursus mattis molestie a iaculis at. Velit ut tortor pretium viverra suspendisse potenti. Cum sociis natoque penatibus et magnis dis parturient montes. Orci nulla

pellentesque dignissim enim sit amet. Dui nunc mattis enim ut.

Placerat orci nulla pellentesque dignissim enim sit amet venenatis. Feugiat in ante metus dictum at tempor. Interdum posuere lorem ipsum dolor sit amet consectetur adipiscing. Viverra vitae congue eu consequat ac felis donec et odio. Augue neque gravida in fermentum et sollicitudin ac. Justo eget magna fermentum iaculis eu non diam phasellus vestibulum. Imperdiet dui accumsan sit amet nulla. Sed id semper risus in hendrerit gravida rutrum quisque non. Turpis egestas pretium aenean pharetra. Pulvinar elementum integer enim neque. Amet purus gravida quis blandit turpis cursus in. In hac habitasse platea dictumst quisque sagittis purus. Amet nulla facilisi morbi tempus iaculis urna. Bibendum at varius vel pharetra vel turpis nunc. Consectetur lorem donec massa sapien. Mauris vitae ultricies leo integer malesuada.

Scope. Blah blah blah.

Contributions. Our primary contributions are as follows.

1. Blah blah blah.
2. Blah blah blah.
3. Blah blah blah.

Chapter 2

Background

This chapter introduces to bitcoin, the world of cryptocurrency and marketplaces. It describes as well what is a proof of solvency, and some of its evolution and current state.

2.1 Bitcoin

Bitcoin is recognized as the world's first successful cryptocurrency and decentralized digital currency. The goal of Bitcoin is to allow financial transactions to be settled without the need of a financial institution. Transactions can occur within 2 participants of the network in realtime, without any middleman. All transactions are settled on a public blockchain, which means that everything can be verified by everyone.

2.1.1 How does Bitcon works

–¿

Transactions

For every participant of the network, there is a public key, a private key and a wallet address. The public key is derived from the private key using elliptic curve multiplication, and the wallet address is derived from the public key using a hashing function. Both are one way function, meaning you cannot derived the other way around. The wallet address can be sean as a bank account number. When you send bitcoin to someone, you send it to their wallet address. To be able to send some bitcoin, you need to sign your transaction. Since transactions are sent on the network, we need to make sure a transaction originates from the sender. The way to do that is to sign your transaction. The digital signature is created from the transaction data and the private key, which is only known by the owner of the address. The public key is then used to make sure that the signature originates from the right private key. Sending a transaction is the easiest problem to solve. The real challenge is to keep track of who owns what, and to avoid the double spending problem. The way to do that is to keep the history of every single transactions. Bitcoin is a blockchain. The blockchain is made of blocks, and the transactions are filling these blocks.

Network

The challenge of the network, is to have every single node agree on the transaction history. Nodes are computers connected to the network, working on publishing new blocks. The nodes work together to agree on the order of transactions. Every new transaction is broadcaseed to all nodes. The nodes puts the transactions into a block, and try to publish that block. In order to publish a block, each node need to solve a proof-of-work challenge. When a node solves the challenge, it broadcasts the block to every nodes. The nodes accepts the block if all transactions are valid. Their is no formal way of approving a new block. A node show its acceptance by starting to work on a new block using the hash of the accepted block as previous hash. Some nodes might accept different blocks, depending on what time they received new blocks. To solve the issue of multiple chains, the longest chain is consideredto be the correct one. If two chains have the same length, nodes keep working on their respective chains untill one of the chains receive a new block, breaking the tie.

Proof-of-work

In order to submit a new block, a node have to find a hash with x number of leading 0 bits. It is exponentially more difficult every time you add a zero. The way to have different hash values, is to change the block timestamp, and the nonce value. The nonce value is there solely for that purpose. Once a block is published, you cannot change any value inside of it because the hash value would change. You would need to redo all the work to find a new good hash. Older blocks are even more secured,

because in order to change the 2nd to last block, you would need to redo the work for the 2 latest blocks. This is the same for every block down the road. The longest chanin is determined by the greatest proof-of-work invest in it. If their is a majority of honest nodes, that chain will grow up the fastest. The difficulty of the new block is determined by an average, in order to generate blocks at a steady pace.

Merkle Tree

Only the merkle root is stored in the block header. When a block is enough in the past, nodes start to only keep block headers in memory. They do not keep the rest of the block. This is why the hash of a block is the hash of the block header, and not the whole block. To keep the integrity of the chain. The merkle root is the top of the Merkle Tree. A merkle tree is a tree where the parent node is the hash of the child nodes.

2.1.2 Why do we need Bitcoin

2.2 Marketplaces

2.3 Zero Knowledge

2.4 Proof of solvency

Scope. Blah blah blah.

Chapter 3

Recursion proofs

Chapter 4

Proof of liabilities

Bibliography

[1] O. Aciiçmez, W. Schindler, and Ç. K. Koç. Improving Brumley and Boneh timing attack on unprotected SSL implementations. In *CCS*, 2005.

[2] A. Acquisti. Receipt-free homomorphic elections and write-in ballots. Technical report, IACR Eprint Report 2004/105, 2004.

[3] A. Adelsbach, S. Gajek, and J. Schwenk. Visual spoofing of SSL protected web sites and effective countermeasures. In *ISPEC*, 2005.

[4] M. Adham. Govchain: An approach to a distributed, equitable government ledger secured by its constituents. Technical report, BitAccess, 2017.

[5] B. Adida. Helios: web-based open-audit voting. In *USENIX Security Symposium*, pages 335–348, 2008.

[6] B. Adida, O. d. Marneffe, O. Pereira, and J.-J. Quisquater. Electing a university president using open-audit voting: Analysis of real-world use of Helios. In *EVT/WOTE*, 2009.

[7] B. Adida and C. A. Neff. Ballot casting assurance. In *EVT*, 2006.

[8] B. Adida and C. A. Neff. Efficient receipt-free ballot casting resistant to covert channels. In *EVT/WOTE*, 2009.

[9] B. Adida and R. L. Rivest. Scratch & Vote: self-contained paper-based cryptographic voting. In *ACM WPES*, pages 29–40, 2006.

[10] R. Aditya, C. Boyd, E. Dawson, and K. Viswanathan. Secure e-voting for preferential elections. In *EGOV*, 2003.

[11] R. Aditya, B. Lee, C. Boyd, and E. Dawson. An efficient mixnet-based voting scheme providing receipt-freeness. In *TrustBus*, 2004.

[12] G. Aggarwal, E. Bursztein, C. Jackson, and D. Boneh. An analysis of private browsing modes in modern browsers. In *USENIX Security*, 2010.

[13] R. Aggarwal and G. Wu. Stock market manipulation—theory and evidence. *Journal of Business*, 79(4), 2003.

[14] D. Ahmad. Two years of broken crypto. *IEEE Security and Privacy*, 6(5), 2008.

[15] L. v. Ahn, M. Blum, N. Hopper, and J. Langford. CAPTCHA: Using hard AI problems for security. In *EUROCRYPT*, 2003.

[16] L. v. Ahn, A. Bortz, N. J. Hopper, and K. O'Neill. Selectively traceable anonymity. In *PET*, 2006.

[17] M. Al-Bassam. Scpki: A smart contract-based pki and identity system. In *ACM BCC*, pages 35–40. ACM, 2017.

[18] N. J. AlFardan and K. G. Paterson. Lucky thirteen: Breaking the TLS and DTLS record protocols. In *IEEE Symposium on Security and Privacy*, 2013.

[19] M. Ali, J. C. Nelson, R. Shea, and M. J. Freedman. Blockstack: A global naming and storage system secured by blockchains. In *USENIX ATC*, pages 181–194, 2016.

[20] R. Ali, J. Barrdear, R. Clews, and J. Southgate. Innovations in payment technologies and the emergence of digital currencies. Quarterly bulletin, Bank of England, 2014.

[21] M. Alicherry and A. D. Keromytis. Doublecheck: Multi-path verification against man-in-the-middle attacks. In *ISCC*, 2009.

[22] B. Amann, M. Vallentin, S. Hall, and R. Sommer. Revisiting SSL: A large-scale study of the internet's most trusted protocol. Technical report, ICSI, 2012.

[23] A. Ambainis, M. Jakobsson, and H. Lipmaa. Cryptographic randomized response techniques. *PKC*, 2004.

[24] C. Amrutkar, P. Traynor, and P. van Oorschot. Measuring SSL indicators on mobile browsers: Extended life or end of the road? In *ISC*, 2012.

[25] R. Anderson and M. Kuhn. Tamper resistance: A cautionary note. In *Proceedings of the 2nd Conference on Proceedings of the Second USENIX Workshop on Electronic Commerce - Volume 2*, 1996.

[26] R. J. Anderson and E. Biham. Two practical and provably secure block ciphers: BEARS and LION. In *FSE*, 1996.

[27] R. J. Anderson, R. M. Needham, and A. Shamir. The steganographic file system. In *IH*, 1998.

[28] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In *Financial Cryptography*, 2013.

[29] S. Ansolabehere. Guide to the 2008 cooperative congressional election survey. Technical report, M.I.T., 2009.

[30] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster. Building a dynamic reputation system for DNS. In *USENIX Security*, 2010.

[31] X. Ao, N. H. Minsky, and V. Ungureanu. Formal treatment of certificate revocation under communal access control. In *IEEE Symposium on Security and Privacy*, 2001.

[32] A. W. Appel, M. Ginsburg, H. Hursti, B. W. Kernighan, C. D. Richards, G. Tan, and P. Venetis. The new jersey voting-machine lawsuit and the avc advantage dre voting machine. In *EVT/WOTE*, 2009.

[33] R. Araujo, R. F. Custodio, and J. v. Graaf. A verifiable voting protocol based on Farnel. In *WOTE*, 2006.

[34] R. Araujo, R. F. Custodio, and J. v. Graaf. A verifiable voting protocol based on Farnel. In *Towards Trustworthy Elections*, volume 6000 of *LNCS*. Springer, 2010.

[35] R. Araujo, S. Foulle, and J. Traoré. A practical and secure coercion-resistant scheme for remote elections. In *Frontiers of Electronic Voting*, 2007.

[36] R. Araujo, S. Foulle, and J. Traoré. A practical and secure coercion-resistant scheme for internet voting. *Toward Trustworthy Elections*, LNCS 6000, 2010.

[37] R. Araujo, N. B. Rajeb, R. Robbana, J. Traoré, and S. Yousfi. Towards practical and secure coercion-resistant electronic elections. In *CANS*, 2010.

[38] R. Araujo and P. Y. A. Ryan. Improving the Farnel voting scheme. In *EVOTE*, 2008.

[39] K. J. Arrow, R. Forsythe, M. Gorham, R. Hahn, R. Hanson, J. O. Ledyard, S. Levmore, R. Litan, P. Milgrom, F. D. Nelson, G. R. Neumann, M. Ottaviani, T. C. Schelling, R. J. Shiller, V. L. Smith, E. Snowberg, C. R. Sunstein, P. C. Tetlock, P. E. Tetlock, H. R. Varian, J. Wolfers, and E. Zitzewitz. The promise of prediction markets. *Science*, 320(5878), 2008.

[40] G. Ateniese and S. Mangard. A new approach to DNS security (DNSSEC). In *CCS*, 2001.

[41] T. Aura, P. Nikander, and G. Camarillo. Effects of mobility and multihoming on transport-protocol security. In *IEEE Symposium on Security and Privacy*, 2004.

[42] T. Aura, P. Nikander, and J. Leiwo. DoS-resistant authentication with client puzzles. In *Security Protocols*, 2000.

[43] A. Aviv, P. Cerny, S. Clark, E. Cronin, G. Shah, M. Sherr, and M. Blaze. Security evaluation of ES&S voting machines and election management system. In *EVT*, pages 1–13, 2008.

[44] L. Babai. Trading group theory for randomness. In *ACM STOC*, 1985.

[45] L. Babai and S. Moran. Arthur-merlin games: a randomized proof system, and a hierarchy of complexity class. *J. Comput. Syst. Sci.*, 36(2):254–276, 1988.

[46] A. Back. Hashcash: a denial of service counter-measure, 2002.

[47] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille. Enabling blockchain innovations with pegged sidechains. Technical report, 2014.

[48] L. C. Baird, M. E. Harmon, R. R. Young, and J. E. Armstrong. Apparatus and method for authenticating access to a network resource. United States Patent, 6732278, 2004.

[49] Implications for central banks of the development of electronic money. Technical report, Bank for International Settlements, 1996.

[50] Digital currencies. Technical report, Bank for International Settlements and Committee on Payments and Market Infrastructures, 2015.

[51] Cross-border interbank payments and settlements. Technical report, Bank of Canada, Bank of England, and Monetary Authority of Singapore, Nov. 2018.

[52] Enabling cross-border High Value Transfer Using Distributed Ledger Technologies. Technical report, Bank of Canada, Monetary Authority of Singapore, Accenture, and J.P. Morgan, 2019.

[53] Contingency planning for a central bank digital currency. Technical report, Bank of Canada, 2020.

[54] Central bank digital currency: Opportunities, challenges and design. Discussion paper, Bank of England, 2020.

[55] A. Baraani-Dastjerdi, J. Pieprzyk, and R. Safavi-Naini. A practical electronic voting protocol using threshold schemes. In *ACSAC*, 1995.

[56] B. Barak and S. Halevi. A model and architecture for pseudo-random generation and applications to `/dev/random`. In *ACM CCS*, 2005.

[57] G. Bard. The vulnerability of SSL to chosen-plaintext attack. Technical Report 2004/111, IACR ePrint, 2004.

[58] G. V. Bard. A challenging but feasible blockwise-adaptive chosen-plaintext attack on SSL. In *SECRYPT*, 2006.

[59] G. V. Bard. Spelling-error tolerant, order-independent pass-phrases via the Damerau-Levenshtein string-edit distance metric. In *AISW*, 2007.

[60] E. Barker and A. Roginsky. Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths. Special Publication 800-131A, NIST, 2011.

[61] C. Barontini and H. Holden. Proceeding with caution: A survey on central bank digital currency. Technical report, Bank for International Settlements, 2019.

[62] A. Barth, J. Caballero, and D. Song. Secure content sniffing for web browsers, or how to stop papers from reviewing themselves. In *IEEE Symposium on Security and Privacy*, 2009.

[63] J. J. Bartholdi and J. B. Orlin. Single transferable vote resists strategic voting. *Social Choice and Welfare*, 8:341–354, 1991.

[64] D. Basin, S. Radomirovic, and L. Schmid. Alethea: A provably secure random sample voting protocol. In *IEEE CSF*, 2018.

[65] J. Bau and J. Mitchell. A security evaluation of DNSSEC with NSEC3. In *NDSS*, 2010.

[66] M. Baudet, G. Danezis, and A. Sonnino. Fastpay: High-performance byzantine fault tolerant settlement. *arXiv:2003.11506 [cs]*, 2020.

[67] O. Baudron, P.-A. Fouque, D. Pointcheval, G. Poupard, and J. Stern. Practical multi-candidate election system. In *ACM PODC*, 2001.

[68] M. L. Bech and R. Garratt. Central bank cryptocurrencies. *BIS Quarterly Review*, September 2017.

[69] J. Behrens. The origins of liquid democracy. *The Liquid Democracy Journal*, 5, 2017.

[70] M. Bellare. Practice-oriented provable security. In *Lectures on Data Security*. LNCS 1561, 1999.

[71] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *FOCS*, 1997.

[72] L. Bello and M. Bertachhini. Predictable PRNG in the vulnerable Debian OpenSSL package: the what and the how. In *DEFCON 16*, 2008.

[73] S. M. Bellovin and E. Rescorla. Deploying a new hash algorithm. In *NDSS*, 2006.

[74] J. Benaloh. Cryptographic capsules: A disjunctive primitive for interactive protocols. In *CRYPTO*, 1986.

[75] J. Benaloh. Secret sharing homomorphisms: Keeping a secret secret. In *EUROCRYPT*, 1986.

[76] J. Benaloh. *Verifiable secret-ballot elections*. PhD thesis, Yale University, 1987.

[77] J. Benaloh. Simple verifiable elections. In *EVT*, 2006.

[78] J. Benaloh. Ballot casting assurance via voter-initiated poll station auditing. In *EVT*, 2007.

[79] J. Benaloh, T. Moran, L. Naish, K. Ramchen, and V. Teague. Shuffle-sum: Coercion-resistant verifiable tallying for stv voting. *IEEE TIFS*, 4(4):684–698, 2009.

[80] J. Benaloh and D. Tuinstra. Receipt-free secret-ballot elections. In *ACM STOC*, 1994.

[81] J. Benaloh and M. Yung. Distributing the power of a government to enhance the privacy of voters. In *ACM PODC*, 1986.

[82] J. D. Benaloh (*né* Cohen) and M. J. Fisher. A robust and verifiable cryptographically secure election scheme. In *SFCS*, 1985.

[83] I. Bentov, A. Mizrahi, and M. Rosenfeld. Decentralized prediction market without arbiters. In *BITCOIN*, pages 199–217, Cham, 2017. Springer International Publishing.

[84] K. Bhargavan, C. Fournet, R. Corin, and E. Zalinescu. Cryptographically verified implementations for TLS. In *CCS*, 2008.

[85] K. Bhargavan, C. Fournet, R. Corin, and E. Zălinescu. Verified cryptographic implementations for TLS. *ACM TISSEC*, 15(1), 2012.

[86] A. Biryukov, D. Khovratovich, and S. Tikhomirov. Findel: Secure derivative contracts for ethereum. In *WTSC*, Cham, 2017. Springer International Publishing.

[87] A. Biryukov, D. Khovratovich, and S. Tikhomirov. Privacy-preserving kyc on ethereum. In *ERCIM Blockchain Workshop*, 2018.

[88] O. Bjerg. Designing New Money - The Policy Trilemma of Central Bank Digital Currency. Technical report, Copenhagen Business School, CBS, 2017.

[89] F. Black and M. Scholes. The pricing of options and corporate liabilities. *Journal of Political Economy*, 81(3), 1973.

[90] M. Blaze and S. M. Bellovin. Session-layer encryption. In *USENIX Security*, 1995.

[91] M. Blaze, A. Cordero, S. Engle, C. Karlof, N. Sastry, M. Sherr, T. Stegers, and K.-P. Yee. Source code review of the sequoia voting system. In *State of California's Top to Bottom Review*, 2007.

[92] M. Blaze, J. Ioannidis, and A. D. Keromytis. Trust management for IPsec. In *NDSS*, 2001.

[93] M. Blaze, J. Ioannidis, and A. D. Keromytis. Trust management for IPsec. *ACM TISSEC*, 5(2), 2002.

[94] D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In *CRYPTO*, 1998.

[95] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo random number generator. *SIAM J. Comput.*, 15(2):364–383, 1986.

[96] C. Boar, H. Holden, and A. Wadsworth. Impending arrival – a sequel to the survey on central bank digital currency. BIS Papers 107, Bank for International Settlements, 2020.

[97] J. M. Bohli, J. Mueller-Quade, and S. Roehrich. Bingo voting: Secure and coercion-free voting using a trusted random number generator. In *VOTE-ID*, pages 111–124, 2007.

[98] D. Boneh, X. Ding, G. Tsudik, and C. M. Wong. A method for fast revocation of public key certificates and security capabilities. In *USENIX Security*, 2001.

[99] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO*, 2005.

[100] D. Boneh, E.-J. Goh, and K. Nissam. Evaluating 2-DNF formulas on ciphertexts. In *TCC*, 2005.

[101] D. Boneh and P. Golle. Almost entirely correct mixing with applications to voting. In *ACM CCS*, 2002.

[102] J. Bonneau. Ethiks: Using ethereum to audit a coniks key transparency log. In *Financial Cryptography*, pages 95–105. Springer, 2016.

[103] J. Bonneau, J. Clark, and S. Goldfeder. On bitcoin as a public randomness source. Cryptology ePrint Archive, Report 2015/1015, 2015. `https://eprint.iacr.org/2015/1015`.

[104] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In *IEEE Symp. Security & Privacy*, 2012.

[105] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. Kroll, and E. Felten. Bitcoin and second-generation cryptocurrencies. In *IEEE Symposium on Security and Privacy*, 2015.

[106] J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten. Mixcoin: Anonymity for bitcoin with accountable mixes. In *Financial Cryptography*, 2014.

[107] B. Borchert. Segment-based visual cryptography. Technical Report WSI-2007-04, WSI, 2007.

[108] J. Bos. *Practical Privacy*. PhD thesis, Technische Universiteit Eindhoven, 1992.

[109] J. Bos, D. Chaum, and G. Purdy. A voting scheme. Preliminary draft, 1992.

[110] M. Bouchaud, T. Lyons, M. S. Olive, and K. Timsit. Central banks and the future of digital money. Technical report, ConsenSys Solutions, 2020.

[111] F. Boudot. Efficient proofs that a committed number lies in an interval. In *EUROCRYPT*, 2000.

[112] C. Boyd. A new multiple key cipher and an improved voting scheme. In *EUROCRYPT*, 1989.

[113] S. Brands. Rapid demonstration of linear relations connected by boolean operators. In *EUROCRYPT*, 1997.

[114] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37(2):156–189, 1988.

[115] J. Brett. How project libra and covid-19 drove digital dollar idea in congress. *Forbes*, 2020.

[116] A. Broadbent and A. Tapp. Information-theoretically secure voting without an honest majority. In *WOTE*, 2008.

[117] B. Broadbent. Central banks and digital currencies. Speech, Bank of England, 2016.

[118] J. Brown. Betting Markets with Decentralized Resolution and Persistent Reputation using Electronic Cash. private communication, Dec. 2013.

[119] R. Brown. Anderson: The unmaking of mondex. *Computerworld News Wire*, 1997.

[120] B. B. Brumley and N. Tuveri. Remote timing attacks are still practical. In *ESORICS*, 2011.

[121] D. Brumley and D. Boneh. Remote timing attacks are practical. In *USENIX Security*, 2003.

[122] P. Buhler, T. Eirich, M. Steiner, and M. Waidner. Secure password-based cipher suite for TLS. In *NDSS*, 2000.

[123] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *IEEE Symposium on Security and Privacy*, 2018.

[124] K. Butler, W. Enck, H. Hursti, S. McLaughlin, P. Traynor, and P. McDaniel. Systemic issues in the hart intercivic and premier voting systems: Reflections on project everest. In *EVT*, 2008.

[125] J. A. Calandrino, A. J. Feldman, J. A. Halderman, D. Wagner, H. Yu, and W. P. Zeller. Source code review of the Diebold voting system. In *State of California's Top to Bottom Review*, 2007.

[126] J. A. Calandrino, J. A. Halderman, and E. W. Felten. In defense of pseudorandom sample selection. In *EVT*, 2008.

[127] J. Camenisch, M. Drijvers, and M. Dubovitskaya. Practical uc-secure delegatable credentials with attributes and their application to blockchain. In *ACM CCS*, CCS '17, pages 683–699, New York, NY, USA, 2017. ACM.

[128] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich. How to win the clone wars: efficient periodic n-times anonymous authentication. In *ACM CCS*, 2006.

[129] J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *CRYPTO*, 2004.

[130] J. Camenisch and M. Stadler. Proof systems for general statements about discrete logarithms. Technical report, ETH Zurich, 1997.

[131] R. Canetti and R. Gennaro. Incoercible multiparty computation. In *IEEE FOCS*, 1996.

[132] B. Canvel, A. Hiltgen, S. Vaudenay, and M. Vuagnoux. Password interception in a SSL/TSL channel. In *CRYPTO*, 2003.

[133] S. Cao, Y. Yuan, A. D. Caro, K. Nandakumar, K. Elkhiyaoui, and Y. Hu. Decentralized privacy-preserving netting protocol on blockchain for payment systems. In *Financial Cryptography*, 2020.

[134] R. T. Carback. Private Communications, 2008.

[135] R. T. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P. S. Hernson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, A. T. Sherman, and P. L. Vora. Scantegrity II municipal election at Takoma Park: the first E2E binding governmental election with ballot privacy. In *USENIX Security Symposium*, 2010.

[136] R. T. Carback, J. Clark, A. Essex, and S. Popoveniuc. On the independent verification of a Punchscan election. In *Proc. VoComp*, 2007.

[137] M. Carney. The growing challenges for monetary policy in the current international monetary and financial system. Speach, 2019.

[138] J. Chapman, R. Garratt, S. Hendry, A. McCormack, and W. McMahon. Project jasper: Are Distributed Wholesale Payment Systems Feasible Yet? Financial systems review, Bank of Canada, 2017.

[139] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, 1981.

[140] D. Chaum. Blind signatures for untraceable payments. In *CRYPTO*, 1982.

[141] D. Chaum. Blind signatures for untraceable payments. In *CRYPTO*, 1982.

[142] D. Chaum. Elections with unconditionally-secure ballots and disruption equivalent to breaking rsa. In *EUROCRYPT*, 1988.

[143] D. Chaum. Achieving electronic privacy. *Scientific American*, pages 96–101, 1992.

[144] D. Chaum. Surevote: Technical overview. In *WOTE*, 2001.

[145] D. Chaum. Secret-ballot receipts and transparent integrity: Better and less-costly electronic voting at polling places. Technical report, VReceipt, 2002.

[146] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, 2(1):38–47, 2004.

[147] D. Chaum. Random-sample voting. Online, 2012.

[148] D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, and A. T. Sherman. Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *EVT*, 2008.

[149] D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. L. Rivest, P. Y. A. Ryan, E. Shen, A. T. Sherman, and P. L. Vora. Scantegrity ii: end-to-end verifiability by voters of optical scan elections through confirmation codes. *IEEE Transactions on Information Forensics and Security*, 4(4):611–627, 2009.

[150] D. Chaum, I. Damgård, and J. v. Graaf. Multiparty computations ensuring privacy of each party's input and correctness of the result. In *CRYPTO*, 1987.

[151] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. T. Sherman, and P. Vora. Scantegrity: End-to-end voter verifiable optical-scan voting. *IEEE Security and Privacy*, 6(3):40–46, May/June 2008.

[152] D. Chaum and T. P. Pedersen. Wallet databases with observers. In *CRYPTO*, 1992.

[153] D. Chaum, P. Y. A. Ryan, and S. Schneider. A practical voter-verifiable election scheme. In *ESORICS*, 2005.

[154] S. Chen, Z. Mao, Y.-M. Wang, and M. Zhang. Pretty-bad-proxy: An overlooked adversary in browsers' HTTPS deployments. In *IEEE Symposium on Security and Privacy*, 2009.

[155] Y. Chen and D. M. Pennock. Designing markets for prediction. *AI Magazine*, 2010.

[156] R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. M. Johnson, A. Juels, A. Miller, and D. Song. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contract execution. Technical report, CoRR, 2018.

[157] M. Chesney, M. Jeanblanc-Picque, and M. Yor. Brownian excursions and Parisian barrier options. *Advances in Applied Probability*, 29, 1997.

[158] S. Chiasson, P. C. v. Oorschot, and R. Biddle. Graphical password authentication using cued click points. In *ESORICS*, 2007.

[159] S. S. M. Chow, J. K. Liu, and D. S. Wong. Robust receipt-free election system with ballot secrecy and verifiability. In *NDSS*, 2007.

[160] J. Clark. *Democracy Enhancing Technologies: Toward deployable and incoercible E2E elections*. PhD thesis, University of Waterloo, 2011.

[161] J. Clark, J. Bonneau, A. Miller, J. A. Kroll, E. W. Felten, and A. Narayanan. On decentralizing prediction markets and order books. In *WEIS*, 2014.

[162] J. Clark, D. Demirag, and S. Moosavi. Demystifying stablecoins. In *Communications of the ACM*, volume 63, July 2020.

[163] J. Clark and A. Essex. Commitcoin: Carbon dating commitments with bitcoin. In *Financial Cryptography*, 2012.

[164] J. Clark, A. Essex, and C. Adams. Secure and observable auditing of electronic voting systems using stock indices. In *IEEE Canadian Conference on Electrical and Computer Engineering*, 2007.

[165] J. Clark and U. Hengartner. Panic passwords: Authenticating under duress. In *USENIX HotSec*, 2008.

[166] J. Clark and U. Hengartner. On the use of financial data as a random beacon. In *EVT/WOTE*, 2010.

[167] J. Clark and U. Hengartner. Selections: Internet voting with over-the-shoulder coercion-resistance. In *FC*, 2011.

[168] J. Clark, U. Hengartner, and K. Larson. Not-so-hidden information: optimal contracts for undue influence in E2E voting systems. In *VOTE-ID*, 2009.

[169] J. Clark and P. v. Oorschot. SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. In *IEEE Symposium on Security and Privacy*, 2013.

[170] J. Clark, P. C. van Oorschot, and C. Adams. Usability of anonymous web browsing: an examination of tor interfaces and deployability. In *SOUPS*, 2007.

[171] J. Clark, P. C. van Oorschot, S. Ruoti, K. Seamons, and D. Zappala. Securing email: A stakeholder-based analysis. Under Submission.

[172] M. R. Clarkson, S. Chong, and A. C. Myers. Civitas: Toward a secure voting system. In *IEEE Symposium on Security and Privacy*, pages 354–368, 2008.

[173] W. Clarkson, T. Weyrich, A. Finkelstein, N. Heninger, J. A. Halderman, and E. W. Felten. Fingerprinting blank paper using commodity scanners. In *IEEE Symposium on Security and Privacy*, 2009.

[174] C. Coarfa, P. Druschel, and D. S. Wallach. Performance analysis of TLS web servers. *ACM TOCS*, 24(1), 2006.

[175] B. Cœ uré and J. Loh. Central bank digital currencies. Technical report, Bank for International Settlements and Committee on Payments and Market Infrastructures, 2018.

[176] D. A. Cooper. A model of certificate revocation. In *ACSAC*, 1999.

[177] A. Cordero, D. Wagner, and D. Dill. The role of dice in election audits — extended abstract. In *WOTE*, 2006.

[178] R. Cramer, I. Damgård, and J. B. Nielsen. Multiparty computation from threshold homomorphic encryption. In *EUROCRYPT*, 2001.

[179] R. Cramer, I. Damgård, and P. MacKenzie. Efficient zero-knowledge proofs of knowledge without intractability assumptions. In *PKC*, 2000.

[180] R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *CRYPTO*, 1994.

[181] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung. Multi-authority secret-ballot elections with linear work. In *EUROCRYPT*, 1996.

[182] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *EUROCRYPT*, 1997.

[183] R. Cramer and V. Shoup. A practical public key cryptosystem provavly secure against adaptive chosen ciphertext attack. In *CRYPTO*, 1998.

[184] L. F. Cranor and R. K. Cytron. Sensus: A security-conscious electronic polling system for the internet. In *Hawaii International Conference on System Sciences*, 1997.

[185] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün Sirer, D. Song, and R. Wattenhofer. On scaling decentralized blockchains. In *Bitcoin Workshop*, 2016.

[186] R. F. Custodio. Farnel: um protocolo de votacao papel com verificabilidade parcial. In *Simposio Seguranca em Informatica*, 2001.

[187] I. Dacosta, M. Ahamad, and P. Traynor. Trust no one else: Detecting MITM attacks against SSL/TLS without third-parties. In *ESORICS*, 2012.

[188] G. G. Dagher, B. Buenz, J. Bonneau, J. Clark, and D. Boneh. Provisions: Privacy-preserving proofs of solvency for Bitcoin exchanges. In *CCS*, October 2015.

[189] I. Damgård, J. Groth, and G. Salomonsen. The theory and implementation of an electronic voting system. In *Secure Electronic Voting*, 2003.

[190] I. Damgård and M. Jurik. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. In *PKC*, pages 119–136, 2001.

[191] I. Damgård and M. Jurik. Client/server tradeoffs for online elections. In *PKC*, pages 125–140, 2002.

[192] G. Danezis and S. Meiklejohn. Centrally banked cryptocurrencies. In *NDSS*, 2016.

[193] Central bank digital currency in denmark? Technical report, Danmarks Nationalbank, 2017.

[194] S. Darbha and R. Arora. Privacy in cbdc technology. Technical Report 9, Bank of Canda, 2020.

[195] B. Davenport, A. Newberger, and J. Woodward. Creating a secure digital voting protocol for campus elections. Technical report, Princeton, 1996.

[196] D. Dean and A. Stubblefield. Using client puzzles to protect TLS. In *USENIX Security*, 2001.

[197] J. P. Degabriele and K. G. Paterson. Attacking the IPsec standards in encryption-only configurations. In *IEEE Symposium on Security and Privacy*, 2007.

[198] J. P. Degabriele, K. G. Paterson, and G. J. Watson. Provable security in the real world. *IEEE Security and Privacy*, 9(3), 2011.

[199] S. Delaune, S. Kremer, and M. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *CSFW*, 2006.

[200] The future is here Project Ubin: SGD on Distributed Ledger. Technical report, Deloitte and Monetary Authority of Singapore, 2017.

[201] R. DeMillo, N. Lynch, and M. J. Merritt. Cryptographic protocols. In *ACM STOC*, 1982.

[202] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In *CRYPTO*, 1989.

[203] R. Dhamija and J. Tygar. The battle against phishing: Dynamic security skins. In *SOUPS*, 2005.

[204] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *CHI*, 2006.

[205] G. Di Crescenzo. Privacy for the stock market. In *Financial Cryptography*, 2001.

[206] L. Diamond. *The Spirit of Democracy: The Struggle to Build Free Societies Throughout the World*. Times Books, first edition, 2008.

[207] M. Dietz, A. Czeskis, D. Balfanz, and D. S. Wallach. Origin-bound certificates: A fresh approach to strong client authentication for the web. In *USENIX Security*, 2012.

[208] R. Dingledine, N. Mathewson, and P. Syverson. Tor: the second-generation onion router. In *USENIX Security*, 2004.

[209] R. Dingledine, A. Serjantov, and P. Syverson. Blending different latency traffic with alpha-mixing. In *Privacy Enhancing Technologies*, pages 245–257. Springer, 2006.

[210] H. Dobbertin. Crytanalysis of MD5 compress. In *EUROCRYPT (Rump Session Talk)*, 1996.

[211] Y. Dodis, R. Gennaro, J. Hastad, H. Krawczyk, and T. Rabin. Randomness extraction and key derivation using the CBC, Cascade and HMAC modes. In *CRYPTO*, 2004.

[212] Y. Dodis and A. Yampolskiy. A verifiable random function with short proofs and keys. In *PKC*, 2005.

[213] D. Dolev, C. Dwork, O. Waarts, and M. Yung. Perfectly secure message transmission. *Journal of the ACM*, 40(1):17–47, 1993.

[214] T. Duong and J. Rizzo. Here come the $\oplus$ ninjas. In *Ekoparty*, 2011.

[215] R. Durstenfeld. Algorithm 235: Random permutation. *Communications of the ACM*, 7(7):420, 1964.

[216] Z. Durumeric, J. Kasten, M. Bailey, and J. A. Halderman. Analysis of the https certificate ecosystem. In *IMC*, 2013.

[217] C. Dwork and M. Naor. Pricing via processing or combatting junk mail. In *CRYPTO*, 1992.

[218] D. Eastlake. Publicly verifiable nominations committee (nomcom) random selection. RFC 3797, IETF, 2004.

[219] D. Eastlake. Publicly verifiable nomcom random selection. RFC 2777, IETF, 2006.

[220] P. Eckersley and J. Burns. Is the SSLiverse a safe place? In *Chaos Communication Congress*, 2010.

[221] P. Eckersley and J. Burns. An observatory for the SSLiverse. In *DEFCON 18*, 2010.

[222] Election Data Services Inc. Voting equipment summary by type as of 11/07/2006, 2006.

[223] T. Elgamal. A publick key cryptosystem and a signature scheme based on discrete logarithms. In *CRYPTO*, 1984.

[224] Y. Elley, A. Anderson, S. Hanna, S. Mullan, R. Perlman, and S. Proctor. Building certification paths: Forward vs. reverse. In *NDSS*, 2001.

[225] C. Ellison. Ceremony design and analysis. Technical Report 2007/399, IACR ePrint, 2007.

[226] C. M. Ellison. Establishing identity without certification authorities. In *USENIX Security*, 1996.

[227] W. Engert and B. S. C. Fung. Central bank digital currency: Motivations and implications. Technical report, Bank of Canada, 2017.

[228] S. Eskandari, D. Barrera, E. Stobert, and J. Clark. A first look at the usability of Bitcoin key management. In *USEC*, 2015.

[229] S. Eskandari, J. Clark, V. Sundaresan, and M. Adham. On the feasibility of decentralized derivatives markets. In *WTSC*, 2017.

[230] S. Eskandari, S. Moosavi, and J. Clark. Sok: Transparent dishonesty: front-running attacks on blockchain. In *International Conference on Financial Cryptography and Data Security*, pages 170–189. Springer, 2019.

[231] A. Essex, J. Clark, and C. Adams. Aperio: High integrity elections for developing countries. In *WOTE*, 2008.

[232] A. Essex, J. Clark, and C. Adams. Aperio: High integrity elections for developing countries. In *Towards Trustworthy Elections*, volume 6000 of *LNCS*. Springer, 2010.

[233] A. Essex, J. Clark, R. T. Carback, and S. Popoveniuc. Punchscan in practice: an e2e election case study. In *WOTE*, 2007.

[234] A. Essex, J. Clark, R. T. Carback, and S. Popoveniuc. The Punchscan voting system. Technical report, Submission to the *University Voting Systems Competition (VoComp)*, 2007.

[235] A. Essex, J. Clark, and U. Hengartner. Cobra: Toward concurrent ballot authorization for internet voting. In *EVT/WOTE*, 2012.

[236] A. Essex, J. Clark, U. Hengartner, and C. Adams. How to print a secret. In *HotSec*, 2009.

[237] A. Essex, J. Clark, U. Hengartner, and C. Adams. Eperio: Mitigating technical complexity in cryptographic election verification. In *EVT/WOTE*, 2010.

[238] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 26(6), 1985.

[239] S. Fahl, M. Harbach, T. Muders, L. Baumgartner, B. Freisleben, and M. Smith. Why Eve and Mallory love Android: An analysis of Android SSL (in)security. In *CCS*, 2012.

[240] R. Farashahi, R. Pellikaan, and A. Sidorenko. Extractors for binary elliptic curves. *Designs, Codes, and Cryptography*, 49, 2008.

[241] Federal constitutional court of Germany (Bundesverfassungsgericht). Judgement of 3 March 2009 – 2 BvC 3/07, 2 BvC 4/07 – Verfahren über die Wahlprüfungsbeschwerden, 2009.

[242] A. J. Feldman and J. Benaloh. On subliminal channels in encrypt-on-cast voting systems. In *EVT/WOTE*, 2009.

[243] A. P. Felt and D. Wagner. Phishing on mobile devices. In *USEC*, 2007.

[244] E. Felten, D. Balfanz, D. Dean, and D. S. Wallach. Web spoofing: An internet con game. In *NISSC*, 1997.

[245] A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. In *CRYPTO*, pages 186–194, 1986.

[246] A. Fiat and A. Shamir. Witness indistinguishable and witness hiding protocols. In *ACM STOC*, 1990.

[247] Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements. Technical report, Financial Stability Board, 2020.

[248] FIPR. Consultation on the draft code of practice for the investigation of protected electronic information – part III of the regulation of investigatory powers act 2000. FIPR Response to the Home Office, 2006.

[249] K. Fisher, R. T. Carback, and A. T. Sherman. Punchscan system definition. In *WOTE*, 2006.

[250] B. Ford. A liquid perspective on democratic choice. cs.CY 2003.12393, arXiv, 2018.

[251] P.-A. Fouque, G. Poupard, and J. Stern. Sharing decryption in the context of voting or lotteries. In *FC*, 2000.

[252] B. Fox and B. LaMacchia. Certificate revocation: Mechanics and meaning. In *Financial Cryptography*, 1997.

[253] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum. Users' conceptions of web security: A comparative study (short talk). In *CHI*, 2002.

[254] K. Fu, E. Sit, K. Smith, and N. Feamster. Dos and don'ts of client authentication on the web. In *USENIX Security*, 2001.

[255] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In *ASIACRYPT*, pages 244–251, 1992.

[256] E. Fujisaki and T. Okamoto. A practical and provably secure scheme for publicly verifiable secret sharing and its applications. In *EUROCRYPT*, 1998.

[257] J. Furukawa, H. Miyauchi, K. Mori, S. Obana, and K. Sako. An implementation of a universally verifiable electronic voting scheme based on shuffling. In *FC*, 2002.

[258] J. Furukawa, K. Mori, and K. Sako. An implementation of a mix-net based network voting scheme and its use in a private organization. In *Towards Trustworthy Elections*, volume 6000 of *LNCS*. Springer, 2010.

[259] Investigating the impact of global stablecoins. Technical report, G7 Working Group on Stablecoins, 2019.

[260] E. Gabber, M. Jakobsson, Y. Matias, and A. Mayer. Curbing junk e-mail via secure classification. In *Financial Cryptography*, 1998.

[261] E. Gabrilovich and A. Gontmakher. The homograph attack. *Communications of the ACM*, 45(2), 2002.

[262] S. Gajek, M. Manulis, O. Pereira, A.-R. Sadeghi, and J. Schwenk. Universally composable security analysis of TLS. In *ProvSec*, 2008.

[263] S. Gajek, M. Manulis, A.-R. Sadeghi, and J. Schwenk. Provably secure browser-based user-aware mutual authentication over TLS. In *ASIACCS*, 2008.

[264] J. M. Galvin. Public key distribution with secure DNS. In *USENIX Security*, 1996.

[265] F. D. Garcia, G. de Koning Gans, R. Muijrers, P. van Rossum, R. Verdult, R. W. Schreur, and B. Jacobs. Dismantling mifare classic. In *ESORICS*, 2008.

[266] F. D. Garcia, P. v. Rossum, R. Verdult, and R. W. Schreur. Wirelessly pick-pocketing a mifare classic card. In *IEEE Symposium on Security and Privacy*, 2009.

[267] R. W. Gardner, S. Garera, and A. D. Rubin. Coercion resistant end-to-end voting. In *FC*, 2009.

[268] D. Geer. Technical maturity, reliability, implicit taxes, and wealth creation. *login: The magazine of Usenix & Sage*, 26(8), 2001.

[269] R. Gennaro. Achieving independence efficiently and securely. In *ACM PODC*, 1995.

[270] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Secure distributed key generation for discrete-log based cryptosystems. In *EUROCRYPT*, 1999.

[271] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, V. Shmatikov, and D. Boneh. The most dangerous code in the world: validating SSL certificates in non-browser software. In *CCS*, 2012.

[272] A. Gervais, S. Capkun, G. O. Karame, and D. Gruber. On the privacy provisions of bloom filters in lightweight bitcoin clients. In *ACSAC*, 2014.

[273] F. Giesen, F. Kohlar, and D. Stebila. On the security of TLS renegotiation. Technical Report 2012/630, IACR ePrint, 2012.

[274] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *SOSP*, pages 51–68, 2017.

[275] I. Goldberg and D. Wagner. Randomness and the Netscape browser. *Dr. Dobb's Journal*, 1996.

[276] S. Goldwasser and Y. Kalaj. On the (in)security of the Fiat-Shamir paradigm. In *IEEE FOCS*, 2003.

[277] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. In *ACM STOC*, 1986.

[278] R. Gonggrijp, W.-J. Hengeveld, E. Hotting, S. Schmidt, and F. Weidemann. RIES—Rijnland internet election system: A cursory study of published source code. In *VOTE-ID*, 2009.

[279] G. S. Grewal, M. D. Ryan, S. Bursuc, and P. Y. A. Ryan. Caveat coercitor: Coercion-evidence in electronic voting. In *IEEE Symposium on Security and Privacy*, 2013.

[280] I. Grigg. An open audit of an open certification authority. In *LISA (invited talk)*, 2008.

[281] J. Groth. Efficient maximal privacy in boardroom voting and anonymous broadcast. In *FC*, 2004.

[282] J. Groth. Review of RIES. Technical report, Cryptomathic, 2004.

[283] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT*, 2008.

[284] J. Groth and G. Salomonsen. Strong privacy protection in electronic voting. Technical Report RS-04-13, BRICS, 2004.

[285] W. Gu, A. Raghuvanshi, and D. Boneh. Empirical measurements on pricing oracles and decentralized governance for stablecoins. In *Cryptoeconomic Systems*, 2020.

[286] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais. Sok: Layer-two blockchain protocols. In *Financial Cryptography*, 2020.

[287] L. Gudgeon, D. Perez, D. Harz, B. Livshits, and A. Gervais. The decentralized financial crisis. In *CVCBT*, 2020.

[288] L. Gudgeon, S. M. Werner, D. Perez, and W. J. Knottenbelt. Defi protocols for loanable funds: Interest rates, liquidity and market efficiency. Technical report, arXiv, 2020.

[289] V. Gupta, D. Steblia, S. Fung, S. C. Shantz, N. Gura, and H. Eberle. Speeding up secure web transactions using elliptic curve cryptography. In *NDSS*, 2004.

[290] P. Gutmann. Plug-and-play PKI: A PKI your mother can use. In *USENIX Security*, 2003.

[291] S. Haber and W. S. Stornetta. How to time-stamp a digital document. In *CRYPTO*, 1990.

[292] S. A. Haber and W. S. Stornetta. Secure names for bit-strings. In *CCS*, 1997.

[293] J. A. Halderman and B. Waters. Harvesting verifiable challenges from oblivious online sources. In *ACM CCS*, 2007.

[294] J. L. Hall. On improving the uniformity of randomness with alameda county's random selection process. Technical report, UC Berkeley, 2008.

[295] R. Hansen and J. Sokol. HTTPS can byte me. In *Black Hat USA*, 2010.

[296] R. Hanson. Combinatorial information market design. *Information Systems Frontiers*, 5(1), 2003.

[297] L. Harris. *Trading and exchanges: market microstructure for practitioners*. Oxford, 2003.

[298] J. M. Hayes. The problem with multiple roots in web browswers - certificate masquerading. In *IEEE WETICE*, 1998.

[299] C. Hazay and Y. Lindell. *Efficient Secure Two-Party Protocols*. Springer, 2010.

[300] C. He, M. Sundararajan, A. Datta, A. Derek, and J. C. Mitchell. A modular correctness proof of IEEE 802.11i and TLS. In *CCS*, 2005.

[301] J. Heather and D. Lundin. The append-only web bulletin board. In *FAST*, 2008.

[302] J. Heather, P. Y. A. Ryan, and V. Teague. Pretty good democracy for more expressive voting schemes. In *ESORICS*, 2010.

[303] S. Heiberg, H. Lipmaa, and F. v. Laenen. On e-vote integrity in the case of malicious voter computers. In *ESORICS*, 2010.

[304] J. Helbach and J. Schwenk. Secure internet voting with code sheets. In *VOTE-ID*, 2007.

[305] J. Helbach, J. Schwenk, and S. Schage. Code voting with linkable group signatures. In *EVOTE*, 2008.

[306] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In *USENIX Security*, 2012.

[307] K. Henry, D. R. Stinson, and J. Sui. The effectiveness of receipt-based attacks on threeballot. *IEEE TIFS*, 4(4):699–707, 2009.

[308] M. A. Herschberg. Secure electronic voting over the world wide web. Master's thesis, MIT, 1997.

[309] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: how to cope with perpetual leakage. In *CRYPTO*, 1995.

[310] A. Herzberg and H. Shulman. Stealth DoS attacks on secure channels. In *NDSS*, 2010.

[311] A. Hess, J. Jacobson, H. Mills, R. Wamsley, K. E. Seamons, and B. Smith. Advanced client/server authentication in TLS. In *NDSS*, 2002.

[312] M. Hirt. *Multi-Party Computation: Efficient Protocols, General Adversaries and Voting*. PhD thesis, ETH Zurich, 2001.

[313] M. Hirt. Receipt-free K-out-of-L voting based on ElGamal encryption. In *Towards Trustworthy Elections*, volume 6000 of *LNCS*. Springer, 2010.

[314] M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In *EUROCRYPT*, 2000.

[315] R. Holz, L. Braun, N. Kammenhuber, and G. Carle. The SSL landscape: A thorough analysis of the X.509 PKI using active and passive measurements. In *IMC*, 2011.

[316] P. Horster, M. Michels, and H. Petersen. Blind multisignature schemes and their relevance to electronic voting. In *ACSAC*, 1995.

[317] L.-S. Huang, E. Y. Chen, A. Barth, E. Rescorla, and C. Jackson. Talking to yourself for fun and profit. In *W2SP*, 2011.

[318] M. A. Huang and S. Teng. Secure and verifiable schemes for election and general distributed computing problems. In *ACM PODC*, 1988.

[319] E. Hubbers, B. Jacobs, and W. Pieters. Ries: Internet voting in action. In *Computer Software and Applications Conference (COMPSAC)*, pages 417–424, 2005.

[320] E. Hubbers, B. Jacobs, B. Schoenmakers, H. van Tilborg, and B. de Weger. Description and analysis of the RIES internet voting system. Technical report, Eindhoven Institute for the Protection of Systems and Information (EiPSI), 2008.

[321] S. Inguva, E. Rescorla, H. Shacham, , and D. S. Wallach. Source code review of the Hart InterCivic voting system. In *State of California's Top to Bottom Review*, 2007.

[322] C. Jackson and A. Barth. Beware of finer-grained origins. In *W2SP*, 2008.

[323] C. Jackson and A. Barth. ForceHTTPS: Protecting high-security web sites from network attacks. In *WWW*, 2008.

[324] C. Jackson, A. Barth, A. Bortz, W. Shao, and D. Boneh. Protecting browsers from dns rebinding attacks. In *CCS*, 2007.

[325] C. Jackson, D. R. Simon, D. S. Tan, and A. Barth. An evaluation of extended validation and picture-in-picture phishing attacks. In *USEC*, 2007.

[326] M. Jacobsson, A. Juels, and R. L. Rivest. Making mix nets robust for electronic voting by randomized partial checking. In *USENIX Security Symposium*, pages 339–353, 2002.

[327] T. Jager, F. Kohlar, S. Schäge, and J. Schwenk. On the security of TLS-DHE in the standard model. In *CRYPTO*, 2012.

[328] M. Jakobsson and A. Juels. Proofs of work and bread pudding protocols. In *Communications and Multimedia Security*, 1999.

[329] M. Jakobsson and A. Juels. Mix and match: Secure function evaluation via ciphertexts. In *ASIACRYPT*, 2000.

[330] M. Jakobsson, K. Sako, and R. Impagliazzo. Designated verifier proofs and their applications. In *EUROCRYPT*, 1996.

[331] M. Jakobsson, E. Stolterman, S. Wetzel, and L. Yang. Love and authentication. In *CHI*, 2008.

[332] J. Jarmoc. SSL/TLS interception proxies and transitive trust. In *Black Hat Europe*, 2012.

[333] D. Jefferson, E. Ginnold, K. Midstokke, K. Alexander, P. Stark, and A. Lehmkuhl. Evaluation of audit sampling models and options for strengthening California's manual count. Technical report, State of California's Post-Election Audit Standards Working Group, 2007.

[334] T. Jim. SD3: a trust management system with certified evaluation. In *IEEE Symposium on Security and Privacy*, 2001.

[335] R. Joaquim and C. Ribeiro. Codevoting: protection against automatic vote manipulation in an uncontrolled environment. In *VOTE-ID*, 2007.

[336] R. Joaquim, C. Ribeiro, and P. Ferreira. Veryvote: A voter verifiable code voting system. In *VOTE-ID*, 2009.

[337] R. Joaquim, C. Ribeiro, and P. Ferreira. Improving remote voting security with CodeVoting. In *Towards Trustworthy Elections*, volume 6000 of *LNCS*. Springer, 2010.

[338] J. P. Jones, D. F. Berger, and C. V. Ravishankar. Layering public key distribution over secure DNS using authenticated delegation. In *ACSAC*, 2005.

[339] J. Jonsson and B. S. Kaliski Jr. On the security of RSA encryption in TLS. In *CRYPTO*, 2002.

[340] M. Joye and M. Tunstall. Securing OpenSSL against micro-architectural attacks. In *SECRYPT*, 2007.

[341] J.p. morgan creates digital coin for payments. Technical report, J.P. Morgan, 2019.

[342] A. Juels and J. Brainard. Client puzzles: A cryptographic defense against connection depletion attacks. In *NDSS*, 1999.

[343] A. Juels, D. Catalano, and M. Jacobsson. Coercion-resistant electronic elections. In *ACM WPES*, 2005.

[344] A. Juels and M. Jakobsson. Coercion-resistant electronic elections. Technical report, Citeseer, 2002.

[345] A. Juels, M. Jakobsson, E. Shriver, and B. Hillyer. How to turn loaded dice into fair coins. *IEEE Transactions on Information Theory*, 46(3), 2000.

[346] A. Juškaitė, S. Šiaudinis, and T. Reichenbachas. CBDC — in a whirlpool of discussion. Occasional paper series, Lietuvos bankas, 2019.

[347] B. Kaliski. Pkcs #5: Password-based cryptography specification. RFC 2898, 2000. http://tools.ietf.org/html/rfc2898.

[348] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten. Arbitrum: Scalable, private smart contracts. In *USENIX Security*, 2018.

[349] H. A. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan. An empirical study of namecoin and lessons for decentralized namespace design. In *WEIS*. Citeseer, 2015.

[350] D. Kaminsky. Black Ops 2008: it's the end of the cache as we know it. In *Black Hat USA*, 2008.

[351] D. Kaminsky, M. L. Patterson, and L. Sassaman. PKI layer cake: New collision attacks against the global X.509 infrastructure. In *Financial Cryptography*, 2010.

[352] C. Kane. Voting and verifiability: interview with Ron Rivest. *RSA Vantage Magazine*, 7(1), 2010.

[353] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn. An empirical analysis of anonymity in zcash. In *USENIX Security*, 2018.

[354] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: A systems perspective. In *USENIX Security Symposium*, 2005.

[355] C. Karlof, N. Sastry, and D. Wagner. The promise of cryptographic voting protocols. Technical report, Berkeley, 2005.

[356] C. Karlof, J. Tygar, and D. Wagner. Conditioned-safe ceremonies and a user study of an appplication to web authentication. In *NDSS*, 2009.

[357] A. H. Karp, M. Stiegler, and T. Close. Not one click for security. Technical Report HPL-2009-53, HP Labs, 2009.

[358] T. Kasper, M. Silbermann, and C. Paar. All you can eat or breaking a real-world contactless payment system. In *Financial Cryptography*, 2010.

[359] J. Katz. Efficient and non-malleable proofs of plaintext knowledge and applications. In *EUROCRYPT*, 2003.

[360] J. Katz. Universally composable multi-party computation using tamper-proof hardware. In *EUROCRYPT*, pages 115–128, 2007.

[361] J. Keller and J. Kilian. A linked-list approach to cryptographically secure elections using instant runoff voting. In *ASIACRYPT*, 2008.

[362] J. Kelsey. Compression and information leakage of plaintext. In *FSE*, 2002.

[363] J. Kelsey, A. Regenscheid, T. Moran, and D. Chaum. Attacking paper-based E2E voting systems. In *Towards Trustworthy Elections*, volume 6000 of *LNCS*, pages 370–387. Springer, 2010.

[364] A. Kiayias and M. Yung. Self-tallying elections and perfect ballot secrecy. In *PKC*, pages 141–158, 2002.

[365] A. Kiayias and M. Yung. The vector-ballot e-voting approach. In *FC*, 2004.

[366] A. Kiayias and M. Yung. The vector-ballot approach for online voting procedures. In *Towards Trustworthy Elections*, volume 6000 of *LNCS*, pages 155–174. Springer, 2010.

[367] K. Kim. Killer application of pki to internet voting. In *International Workshop for Asia Public Key Infrastructures*, 2002.

[368] A. Klages-Mundt and A. Minca. While stability lasts: A stochastic model of stablecoins. Technical report, arXiv, 2020.

[369] R. Koenig, R. Haenni, and S. Fischli. Preventing board flooding attacks in coercion-resistant electronic voting schemes. In *SEC*, 2011.

[370] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *IEEE Symposium on Security and Privacy*, 2004.

[371] J. Koning. Fedcoin: A central bankissued cryptocurrency. Technical report, R3 Reports, 2016.

[372] J. G. Koppella and J. A. Steena. The effects of ballot position on election outcomes. *The Journal of Politics*, 66(1):267–281, 2004.

[373] P. Koshy, D. Koshy, and P. McDaniel. An analysis of anonymity in bitcoin using p2p network traffic. In *Financial Cryptography*, 2014.

[374] H. Krawczyk. The order of encryption and authentication for protecting communications (or: how secure is SSL?). In *CRYPTO*, 2001.

[375] H. Krawczyk. Cryptographic extraction and key derivation: The HKDF scheme. In *CRYPTO*, 2010.

[376] T. Krivoruchko. Robust coercion-resistant registration for remove e-voting. In *WOTE*, 2007.

[377] O. Kulyk, S. Neumann, K. Marky, J. Budurushi, and M. Volkamer. Coercion-resistant proxy voting. *Computers & Security*, 71, 2017.

[378] A. Kumar, C. Fischer, S. Tople, and P. Saxena. A traceability analysis of monero's blockchain. In *ESORICS*, 2017.

[379] R. Kusters and T. Truderung. An epistemic approach to coercion-resistance for electronic voting protocols. In *IEEE Symposium on Security and Privacy*, 2009.

[380] R. Kusters, T. Truderung, and A. Vogt. Improving and simplifying a variant of pret a voter. In *VOTE-ID*, 2009.

[381] R. Kusters, T. Truderung, and A. Vogt. Accountability: Definition and relationship to verifiability. In *ACM CCS*, 2010.

[382] R. Kusters, T. Truderung, and A. Vogt. A game-based definition of coercion-resistance and its application. In *CSF*, 2010.

[383] R. Kusters, T. Truderung, and A. Vogt. Proving coercion-resistance of Scantegrity II. In *ICICS*, 2010.

[384] M. Kutylowski and F. Zagorski. Verifiable internet voting solving secure platform problem. In *IWSEC*, 2007.

[385] T. Lane. Money and payments in the digital age. Technical report, Bank of Canada, 2020.

[386] A. Langley. Beyond the basics of HTTPS serving. *USENIX ;Login:*, Dec 2011.

[387] T. Latter. The choice of exchange rate regime. Handbooks in central banking, Centre for Central Banking Studies, Bank of England, 1996.

[388] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. In *ICISC*, 2003.

[389] B. Lee and K. Kim. Receipt-free electronic voting through collaboration of voter and honest verifier. In *JS-ISC*, 2000.

[390] B. Lee and K. Kim. Receipt-free electronic voting scheme with a tamper-resistant randomizer. In *ICISC*, 2002.

[391] H. K. Lee, T. Malkin, and E. Nahum. Cryptographic strength of SSL/TLS servers: Current and recent practices. In *IMC*, 2007.

[392] S. Lefranc and D. Naccache. Cut-&-paste attacks with JAVA. In *ICISC*, 2002.

[393] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter. Public keys. In *CRYPTO*, 2012.

[394] R. Leshner and G. Hayes. Compound: The money market protocol. Technical report, Compound Finance, 2018.

[395] C. Lesniewski-Laas and M. F. Kaashoek. SSL splitting: securely serving data from untrusted caches. In *USENIX Security*, 2003.

[396] J. Li and X. Kang. mSSL: Extending SSL to support data sharing among collaborative clients. In *ACSAC*, 2005.

[397] M. Liberatore and B. N. Levine. Inferring the source of encrypted HTTP connections. In *CCS*, 2006.

[398] H. Lipmaa. On the CCA1-security of Elgamal and Damgård's Elgamal. In *Inscrypt*, 2010.

[399] F. Liu, C. K. Wu, and X. J. Lin. The alignment problem of visual cryptography schemes. *Designs, Codes and Cryptography*, 50(2), 2009.

[400] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf. Pseudonym systems. In *Selected Areas in Cryptography*, 1999.

[401] E. Magkos, M. Burmester, and V. Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In *I3E*, 2001.

[402] D. Malkhi, O. Margo, and E. Pavlov. E-voting without 'cryptography'. In *FC*, 2002.

[403] T. Mancini Griffoli, M. S. Martinez Peria, I. Agur, A. Ari, J. Kiff, A. Popescu, and C. Rochon. Casting light on central bank digital currencies. IMF Staff Discussion Notes 18/08, International Monetary Fund, 2018.

[404] M. Marlinspike. More tricks for defeating SSL in practice. In *DEFCON 17*, 2009.

[405] M. Marlinspike. New tricks for defeating SSL in practice. In *Black Hat DC*, 2009.

[406] M. Marlinspike. SSL and the future of authenticity. In *Black Hat USA*, 2011.

[407] O. d. Marneffe, O. Pereira, and J.-J. Quisquater. Simulation-based analysis of e2e voting systems. In *VOTE-ID*, 2007.

[408] R. J. Massa, T. R. Ellis, and R. G. LePage. Intelligent surveillance alarm system and method. United States Patent, 4589081, 1986.

[409] F. Massacci, C. N. Ngo, J. Nie, D. Venturi, and J. Williams. Futuresmex: Secure, distributed futures market exchange. In *2018 IEEE Symposium on Security and Privacy (SP)*, 2018.

[410] N. Mavrogiannopoulos, F. Vercauteren, V. Velichkov, and B. Preneel. A cross-protocol attack on the TLS protocol. In *CCS*, 2012.

[411] D. McCarney, D. Barrera, J. Clark, S. Chiasson, and P. C. van Oorschot. Tapas: design, implementation, and usability evaluation of a password manager. In *ACSAC*, 2012.

[412] P. McCorry, E. Heilman, and A. Miller. Atomically trading with roger: Gambling on the success of a hardfork. In *CBT*, pages 334–353, Cham, 2017. Springer International Publishing.

[413] P. McCorry, S. F. Shahandashti, and F. Hao. A smart contract for boardroom voting with maximum voter privacy. In *Financial Cryptography*, 2017.

[414] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. A fistful of bitcoins: characterizing payments among men with no names. In *IMC*, 2013.

[415] B. Meng. A coercion-resistant internet voting protocol. In *ICSNC*, 2007.

[416] R. Merton. Theory of rational option pricing. *Journal of Economics and Management Sciences*, 4(1), 1973.

[417] M. Michels and P. Horster. Some remarks on a receipt-free and universally verifiable mix-type voting scheme. In *ASIACRYPT*, 1996.

[418] I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *IEEE Symposium on Security and Privacy*, 2013.

[419] G. Miller. Note on the bias of information estimates. In *Information Theory in Psychology II-B*. Free Press, 1955.

[420] J. C. Mitchell, V. Shmatikov, and U. Stern. Finite-state analysis of SSL 3.0. In *USENIX Security*, 1998.

[421] N. Modadugu and E. Rescorla. The design and implementation of datagram TLS. In *NDSS*, 2004.

[422] A. Moin, K. Sekniqi, and E. G. Sirer. Sok: A classification framework for stablecoin designs. In *Financial Cryptography*, 2020.

[423] S. Moosavi and J. Clark. Ghazal: toward truly authoritative web certificates using ethereum. In *WTSC*, 2018.

[424] T. Moran and M. Naor. Receipt-free universally-verifiable voting with everlasting privacy. In *CRYPTO*, 2006.

[425] T. Moran and M. Naor. Split-ballot voting: Everlasting privacy with distributed trust. In *ACM CCS*, 2007.

[426] T. Moran and G. Segev. David and goliath commitments: Uc computation for asymmetric parties using tamper-proof hardware. In *EUROCRYPT*, 2008.

[427] P. Morrissey, N. P. Smart, and B. Warinschi. A modular security analysis of the TLS handshake protocol. In *ASIACRYPT*, 2008.

[428] T. Moyer, K. Butler, J. Schiffman, P. McDaniel, and T. Jaeger. Scalable web content attestation. In *ACSAC*, 2009.

[429] R. Mraz. Secure blue: An architecture for a scalable, reliable high volume SSL internet server. In *ACSAC*, 2001.

[430] A. Munje and T. Plestid. Password methods and systems for use on a mobile device. United States Patent (Pending), 11181522, 2007.

[431] A. C. Myers, M. Clarkson, and S. Chong. Civitas: Toward a secure voting system. In *IEEE Symposium on Security and Privacy*, pages 354–368, 2008.

[432] M. Myers. Revocation: Options and challenges. In *Financial Cryptography*, 1998.

[433] S. Nakamoto. Bitcoin: A peer-to-peer electionic cash system. Unpublished, 2008.

[434] M. Naor. Bit commitment using pseudo-randomness (extended abstract). In *CRYPTO*, pages 128–136, 1989.

[435] M. Naor and K. Nissim. Certificate revocation and certificate update. In *USENIX Security*, 1998.

[436] M. Naor and A. Shamir. Visual cryptography. In *EUROCRYPT*, 94.

[437] A. Narayanan, J. Bonneau, E. W. Felten, A. Miller, and S. Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton, 2016.

[438] A. Narayanan and J. Clark. Bitcoin's academic pedigree. *Communications of the ACM*, 60(12), 2017.

[439] N. Narula, W. Vasquez, and M. Virza. zkledger: Privacy-preserving auditing for distributed ledgers. In *USENIX NSDI*, 2018.

[440] N. Narula and L. H. White. Does the u.s. need a national digital currency? *Washington Post*, 2020.

[441] Nasdaq linq enables first-ever private securities issuance documented with blockchain technology. Technical report, NASDAQ, 2015.

[442] Y. Nasser, C. Okoye, J. Clark, and P. Y. A. Ryan. Blockchains and voting: Somewhere between hype and a panacea. Online, 2017.

[443] C. A. Neff. A verifiable secret shuffle and its application to e-voting. In *ACM CCS*, 2001.

[444] C. A. Neff. Practical high certainty intent verification for encrypted votes. Technical report, VoteHere Whitepaper, 2004.

[445] V. Niemi and A. Rendall. How to prevent buying of votes in computer elections. In *ASIACRYPT*, 1994.

[446] H. Nurmi, A. Salomaa, and L. Santean. Secret ballot elections in computer networks. *Computers & Security*, 36(10):553–560, 1991.

[447] M. Ohkubo, F. Miura, M. Abe, A. Fujioka, and T. Okamoto. An improvement on a practical secret voting scheme. In *ISW*, 1999.

[448] K. Ohta. An electrical voting scheme using a single administrator. Technical report, Spring National Convention Record, 1998.

[449] T. Okamoto. Provably secure and practical indentification schemes and corresponding signature schemes. In *CRYPTO*, 1992.

[450] T. Okamoto. An electronic voting scheme. In *IFIP*, 1996.

[451] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In *Workshop on Security Protocols*, 1997.

[452] M. C. Okoye and J. Clark. Ugwo: Toward cryptocurrency lending. In *WTSC*, 2018.

[453] R. Oppliger, R. Hauser, and D. Basin. SSL/TLS session-aware user authentication. *Computer Communications*, 29(12), 2006.

[454] R. Oppliger, J. Schwenk, and C. Lohr. Captcha-based code voting. In *EVOTE*, 2008.

[455] M. Orcutt. The world bank is still loving its blockchain-powered bonds. *MIT Technology Review*, 2019.

[456] Organization for the Advancement of Structured Information Standards (OASIS). Open document format for office applications (opendocument) v1.1, February 2007. http://docs.oasis-open.org/office/v1.1/OS/OpenDocument-v1.1.pdf.

[457] A. Ornaghi and M. Valleri. Man in the middle attacks: demos. In *Black Hat USA*, 2003.

[458] M. J. Osbourne. *An introduction to game theory*. Oxford University Press, 2003.

[459] E. Osterweil, D. Massey, and L. Zhang. Deploying and monitoring DNS security (DNSSEC). In *ACSAC*, 2009.

[460] A. Otsuka and H. Imai. Unconditionally secure electronic voting. In *Towards Trustworthy Elections*, volume 6000 of *LNCS*, pages 107–123. Springer, 2010.

[461] A. Ozment, S. E. Schecter, and R. Dhamija. Web sites should not need to rely on users to secure communications. In *W3C Workshop on Usability and Transparency of Web Authentication*, 2006.

[462] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT*, 1999.

[463] C. Palmer. It's time to fix HTTPS. Online, 2011.

[464] L. Paninski. Estimation of entropy and mutual information. *Neural Computation*, 15, 2003.

[465] C. Park, K. Itoh, and K. Kurosawa. Efficient anonymous channel and all/nothing election scheme. In *EUROCRYPT*, 1993.

[466] S. Park, M. Specter, N. Narula, and R. L. Rivest. Going from bad to worse: From internet voting to blockchain voting. Online, 2020.

[467] B. Parno, C. Kuo, and A. Perrig. Phoolproof phishing prevention. In *Financial Cryptography*, 2006.

[468] L. C. Paulson. Inductive analysis of the internet protocol TLS. *ACM TISSEC*, 1999.

[469] Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement. Technical report, Payments Canada, Bank of Canada and R3, 2017.

[470] T. P. Pedersen. A threshold cryptosystem without a trusted party. In *EUROCRYPT*, 1991.

[471] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *CRYPTO*, pages 129–140, 1992.

[472] K. Peng, R. Aditya, C. Boyd, E. Dawson, and B. Lee. Multiplicative homomorphic e-voting. In *INDOCRYPT*, 2004.

[473] N. J. Percoco and P. Kehrer. Getting SSLizzard. In *DEFCON 19*, 2011.

[474] D. Perez, S. M. Werner, J. Xu, and B. Livshits. Liquidations: Defi on a knife-edge. Technical report, arXiv, 2020.

[475] I. G. A. Pernice, S. Henningsen, R. Proskalovich, M. Florian, and H. Elendner. Monetary stabilization in cryptocurrencies: Design approaches and open questions. In *CVCBT*, 2019.

[476] M. Perry. 365-day: HTTPS cookie stealing. In *DEFCON 16*, 2008.

[477] R. A. Peters. A secure bulletin board. Master's thesis, Technische Universiteit Eindhoven, 2005.

[478] B. Pfitzmann. Breaking an efficient anonymous channel. In *EUROCRYPT*, 1994.

[479] B. Pfitzmann and M. Waidner. Unconditionally untraceable and fault-tolerant broadcast and secret ballot election. Technical report, Institut fur Informatik, Universiat Hildesheim, 1992.

[480] C. Pierrot and B. Wesolowski. Malleability of the blockchain's entropy. *Cryptography and Communications*, 10(1):211–233, Jan 2018.

[481] A. Pilosov and T. Kapela. Stealing the internet: An internet-scale man-in-the-middle attack. In *DEFCON 16*, 2008.

[482] S. Popoveniuc. Speakup: remote unsupervised voting. In *ACNS*, 2010.

[483] S. Popoveniuc, J. Clark, A. Essex, R. T. Carback, and D. Chaum. Securing optical-scan voting. In *Towards Trustworthy Elections*, volume 6000 of *LNCS*. Springer, 2010.

[484] S. Popoveniuc and B. Hosp. An introduction to punchscan. In *WOTE*, 2006.

[485] S. Popoveniuc and P. L. Vora. A framework for secure electronic voting. *Cryptologia*, To appear.

[486] M. Prabhakaran and M. Rosulek. Rerandomizable RCCA encryption. In *CRYPTO*, 2007.

[487] M. Prandini. Efficient certificate status handling within PKIs: an application to public administration services. In *ACSAC*, 1999.

[488] N. Provos. A virtual honeypot framework. In *USENIX Security Symposium*, 2004.

[489] K. Qin, L. Zhou, B. Livshits, and A. Gervais. Attacking the defi ecosystem with flash loans for fun and profit. Technical Report 2003.03810v2, arXiv, 2020.

[490] M. Rabin. Transaction protection by beacons. *Journal of Computer and System Sciences*, 27(2), 1983.

[491] K. Radke, C. Boyd, J. G. Nieto, and M. Brereton. Ceremony analysis: Strengths and weaknesses. In *IFIP SEC*, 2011.

[492] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. In *Security and Privacy in Social Networks*, 2013.

[493] E. Rescorla. *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley, 2001.

[494] E. Rescorla. The internet is too secure already. In *USENIX Security (invited talk)*, 2003.

[495] E. Rescorla. Security holes... who cares? In *USENIX Security*, 2003.

[496] E. Rescorla. Stone knives and bear skins: Why does the internet still run on pre-historic cryptography? In *INDOCRYPT (Invited talk)*, 2006.

[497] E. Rescorla. On the security of election audits with low entropy randomness. In *EVT/WOTE*, 2009.

[498] E. Rescorla, A. Cain, and B. Korver. SSLACC: A clustered SSL accelerator. In *USENIX Security*, 2002.

[499] I. Ristic. Internet SSL survey 2010. In *Black Hat USA*, 2010.

[500] I. Ristic and M. Small. A study of what really breaks SSL. In *Hack in the Box*, 2011.

[501] B. Riva and A. Ta-Shma. Bare-handed electronic voting with pre-processing. In *EVT*, 2007.

[502] R. Rivest. Can we eliminate certificate revocation lists? In *Financial Cryptography*, 1998.

[503] R. L. Rivest and A. Shamir. PayWord and MicroMint: two simple micropayment schemes. In *Security Protocols*, 1996.

[504] R. L. Rivest, A. Shamir, and D. A. Wagner. Time-lock puzzles and timed-release crypto. Technical Report TR-684, MIT, 1996.

[505] R. L. Rivest and W. D. Smith. Three voting protocols: threeballot, VAV, and twin. In *EVT*, 2007.

[506] J. Rizzo and T. Duong. The crime attack. In *Ekoparty*, 2012.

[507] D. Robinson and A. Niemerg. The yield protocol: On-chain lending with interest rate discovery. Technical report, Yield.is, Apr 2020.

[508] K. S. Rogoff. *The Curse of Cash: How Large-Denomination Bills Aid Crime and Tax Evasion and Constrain Monetary Policy*. Princeton University Press, 2017.

[509] D. Ron and A. Shamir. Quantitative Analysis of the Full Bitcoin Transaction Graph. In *Financial Cryptography*, 2013.

[510] B. Rosenberg, editor. *Handbook of Financial Cryptography and Security*. Chapman and Hall/CRC, 2010.

[511] G. Rule. Understanding the central bank balance sheet. Handbooks in Central Banking 32, Centre for Central Banking Studies, 2015.

[512] S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, and R. Cunningham. Blockchain technology: What is it good for? *Communications of the ACM*, 63(1):46–53, 2020.

[513] S. Ruoti, B. Kaiser, A. Yerukhimovich, J. Clark, and R. Cunningham. Blockchain technology: What is it good for? *Communications of the ACM*, 63(1), 2020.

[514] S. Russell. Fast checking of individual certificate revocation on small systems. In *ACSAC*, 1999.

[515] R. K. Russikoff. Computerized password verification system and method for atm transactions. United States Patent, 6871288, 2005.

[516] P. Y. A. Ryan. A variant of the chaum voter-verifiable scheme. Technical Report CS-TR 864, University of Newcastle, 2004.

[517] P. Y. A. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia. Pret a voter: a voter-verifiable voting system. *IEEE TIFS*, 4(4), 2009.

[518] P. Y. A. Ryan and S. A. Schneider. Pret a voter with re-encryption mixes. In *ESORICS*, 2006.

[519] P. Y. A. Ryan and V. Teague. Ballot permutations in pret a voter. In *EVT/WOTE*, 2009.

[520] P. Y. A. Ryan and V. Teague. Pretty good democracy. In *Workshop on Security Protocols*, 2009.

[521] R. Ryan, Z. Anderson, and A. Cheisa. Anatomy of a subway hack. In *DEFCON*, 2008.

[522] K. Sako and J. Kilian. Secure voting using partially compatible homomorphisms. In *CRYPTO*, 1994.

[523] K. Sako and J. Kilian. Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth. In *EUROCRYPT*, pages 393–403, 1995.

[524] K. Sampigethaya and R. Poovendran. A framework and taxonomy for comparison of electronic voting schemes. *Computers & Security*, 25, 2006.

[525] R. Sams. A note on cryptocurrency stabilisation: Seigniorage shares. [Online], 2015.

[526] D. R. Sandler, K. Derr, and D. S. Wallach. VoteBox: a tamper-evident, verifiable electronic voting system. In *USENIX Security Symposium*, 2008.

[527] Sayke. Liquid democracy is not delegative democracy. Blog post, 2006.

[528] S. E. Schecter, R. Dhamija, A. Ozment, and I. Fischer. The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. In *IEEE Symposium on Security and Privacy*, 2007.

[529] C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptography*, 4, 1991.

[530] B. Schoenmakers. A simple publicly verifiable secret sharing scheme and its applications to electronic voting. In *CRYPTO*, 1999.

[531] B. Schoenmakers. Fully auditable electronic secret-ballot elections. *Xootic Magazine*, July 2000.

[532] B. Schoenmakers and P. Tuyls. Practical two-party computation based on the conditional gate. In *ASIACRYPT*, 2004.

[533] M. Schroder. Brownian excursions and Parisian barrier options: a note. *Advances in Applied Probability*, 40(4), 2003.

[534] J. Schweisgut. Coercion-resistant electronic elections with observer. In *EVOTE*, 2006.

[535] A. Serjantov and G. Danezis. Towards an information theoretic metric for anonymity. In *Privacy Enhancing Technologies*, pages 41–53. Springer, 2003.

[536] A. Serjantov, R. Dingledine, and P. Syverson. From a trickle to a flood: Active attacks on several mix types. In *Information Hiding*, pages 36–52. Springer, 2003.

[537] R. U. Seydel. *Tools for computational finance*. Springer, fourth edition, 2009.

[538] Marshall islands to power world's first national digital currency with algorand and sfb technologies'a. Technical report, SFB Technologies, 2020.

[539] H. Shacham and D. Boneh. Fast-track session establishment for TLS. In *NDSS*, 2002.

[540] A. T. Sherman, R. T. Carback, D. Chaum, J. Clark, A. Essex, P. S. Hernson, T. Mayberry, S. Popoveniuc, R. L. Rivest, E. Shen, B. Sinha, and P. L. Vora. Scantegrity mock election at Takoma Park. In *EVOTE*, 2010.

[541] D. Shin and R. Lopes. An empirical study of visual security cues to prevent the SSLstripping attack. In *ACSAC*, 2011.

[542] A. M. Shubina and S. W. Smith. Design and prototype of a coercion-resistant, voter verifiable electronic voting system. In *PST*, 2004.

[543] S. Sinha, N. Gaur, M. Martin, M. Perelman, B. Patel, P. Middleton, P. Ortlieb, K. Lucke, W. Coningsby-Brown, J. Frazer, and J. Bulgin. Retail cbdcs: the next payments frontier. Technical report, OMFIF and IBM, 2020.

[544] M. Smart and E. Ritter. Remote electronic voting with revocable anonymity. In *ISS*, 2009.

[545] D. K. Smetters and G. Durfee. Domain-based administration of identity-based cryptosystems for secure email and IPsec. In *USENIX Security*, 2003.

[546] W. D. Smith. New cryptographic election protocol with best-known theoretical properties. In *Frontiers in Electronic Elections*, 2005.

[547] J. Sobey, R. Biddle, P. van Oorschot, and A. S. Patrick. Exploring user reactions to new browser cues for extended validation certificates. In *ESORICS*, 2008.

[548] C. Soghoian and S. Stamm. Certified lies: Detecting and defeating government interception attacks against SSL. In *Financial Cryptography*, 2011.

[549] S. Son and V. Shmatikov. The hitchhiker's guide to DNS cache poisoning. In *SECURECOMM*, 2010.

[550] D. X. Song, D. Wagner, and X. Tian. Timing analysis of keystrokes and timing attacks on SSH. In *USENIX Security*, 2001.

[551] A. Sotirakopoulos, K. Hawkey, and K. Beznosov. On the challenges in usable security lab studies: Lessons learned from replicating a study on SSL warnings. In *SOUPS*, 2011.

[552] A. Sotirov and M. Zusman. Breaking the security myths of extended validation SSL certificates. In *Black Hat USA*, 2009.

[553] O. Spycher, R. Haenni, and E. Dubuis. Coercion-resistant hybrid voting systems. In *EVOTE*, 2010.

[554] O. Spycher, R. Koenig, R. Haenni, and M. Schlapfer. A new approach towards coercion-resistant remote e-voting in linear time. In *FC*, 2011.

[555] F. Stalder and A. Clement. Exploring policy issues of electronic cash: The mondex case. *Canadian Journal of Communication*, 24(2), 1999.

[556] D. Stebila. Reinforcing bad behaviour: the misuse of security indicators on popular websites. In *OZCHI*, 2010.

[557] M. Stevens, A. Lenstra, and B. de Weger. Chosen-prefix collisions for MD5 and colliding X.509 certificates for different identities. In *EUROCRYPT*, 2007.

[558] M. Stevens, A. Sotirov, J. Appelbaum, A. Lenstra, D. Molnar, D. A. Osvik, and B. de Weger. Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate. In *CRYPTO*, 2009.

[559] C. Stewart. Election technology and the voting experience in 2008. Technical report, VTP Working Paper 71, 2008.

[560] H. Story, B. Harbulot, I. Jacobi, and M. Jones. FOAF+SSL: RESTful authentication for the social web. In *ESWC*, 2009.

[561] Q. Sun, D. R. Simon, Y.-M. Wang, W. Russell, V. N. Padmanabhan, and L. Qiu. Statistical identification of encrypted web browsing traffic. In *IEEE Symposium on Security and Privacy*, 2002.

[562] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: An empirical study of SSL warning effectiveness. In *USENIX Security*, 2009.

[563] J. Surowiecki. Why did criminals trust liberty reserve? *The New Yorker*, 2013.

[564] The riksbank's e-krona project: Report 1. Technical report, Sveriges Riksbank, Sep 2017.

[565] The riksbank's e-krona project: Report 2. Technical report, Sveriges Riksbank, Oct 2018.

[566] E. Syta, I. Tamas, D. Visher, D. I. Wolinsky, P. Jovanovic, L. Gasser, N. Gailly, I. Khoffi, and B. Ford. Keeping authorities" honest or bust" with decentralized witness cosigning. In *IEEE Symposium on Security and Privacy*, pages 526–545. Ieee, 2016.

[567] V. Teague, K. Ramchen, and L. Naish. Coercion resistant tallying for STV voting. In *EVT*, 2008.

[568] C. Thorpe and D. C. Parkes. Cryptographic securities exchanges. In *Financial Cryptography*, 2007.

[569] C. Thorpe and S. R. Willis. Cryptographic rule-based trading. In *Financial Cryptography*, 2012.

[570] Jasper phase III: Securities settlement using distributed ledger technology. Technical report, TMX, R3, Payments Canada, Bank of Canada and Accenture, Oct. 2018.

[571] J. Tobin. A case for preserving regulatory distinctions. *Challenge*, 30(5):10–17, 1987.

[572] E. Topalovic, B. Saeta, L.-S. Huang, C. Jackson, and D. Boneh. Toward short-lived certificates. In *W2SP*, 2012.

[573] Y. Tsiounis and M. Yung. On the security of ElGamal based encryption. In *PKC*, pages 117–134, 1998.

[574] W. G. Tzeng. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters. *IEEE Transactions on Computers*, 53(2), 2004.

[575] United States Election Assistance Commission. The 2008 voluntary voting system guidelines, v1.1), 2009.

[576] D. Unruh and J. Muller-Quade. Universally composable incoercibility. In *CRYPTO*, 2010.

[577] P. C. van Oorschot and M. J. Wiener. Parallel collision search with cryptanalytic applications. *J. Cryptology*, 12:1–28, 1999.

[578] H. R. Varian. System reliability and free riding. In *Economics of Information Security*, volume Advances in Information Security, Volume 12, pages 1–15, 2004.

[579] S. Vaudenay. Security flaws induced by CBC padding: applications to SSL, IPSEC, WTLS, ... In *EUROCRYPT*, 2002.

[580] M. Volkamer and R. Grimm. Multiple casts in online voting: Analyzing chances. In *EVOTE*, 2006.

[581] N. Vratonjic, J. Freudiger, V. Bindschaedler, and J.-P. Hubaux. The inconvenient truth about web certificates. In *WEIS*, 2011.

[582] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol. In *USENIX Workshop on Electronic Commerce*, 1996.

[583] H. J. Wang, C. Grier, A. Moshchuk, S. T. King, P. Choudhury, and H. Venter. The multi-principal OS construction of the Gazelle web browser. In *USENIX Security*, 2009.

[584] X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao, and W. Zhao. Inter-bank payment system on enterprise blockchain platform. In *CLOUD*, 2018.

[585] B. Waters, A. Juels, J. A. Halderman, and E. W. Felten. New client puzzle outsourcing techniques for dos resistance. In *ACM CCS*, pages 246–256, 2004.

[586] S. G. Weber, R. S. d. Araujo, and J. Buchmann. On coercion-resistant electronic elections with linear work. In *ARES*, 2007.

[587] R. Wen and R. Buckland. Masked ballot voting for receipt-free online elections. In *VOTE-ID*, 2009.

[588] R. Wen and R. Buckland. Minimum disclosure counting for the alternative vote. In *VOTE-ID*, 2009.

[589] D. Wendlandt, D. G. Andersen, and A. Perrig. Perspectives: Improving SSH-style host authentication with multi-path probing. In *USENIX Annual Tech*, 2008.

[590] T. Whalen and K. M. Inkpen. Gathering evidence: Use of visual security cues in web browsers. In *Graphics Interface*, 2005.

[591] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon. Passpoints: design and longitudinal evaluation of a graphical password system. *Int. J. Hum.-Comput. Stud.*, 63(1-2):102–127, 2005.

[592] J. Wolfers and E. Zitzewitz. Prediction markets. *Journal of Economic Perspective*, 2004.

[593] J. Wolfers and E. Zitzewitz. Interpreting prediction market prices as probabilities. Technical Report 12200, NBER Working Paper, 2006.

[594] S. Wolfram. *A new kind of science*. Wolfram Media, first edition, 2001.

[595] H. Wu. The misuse of RC4 in microsoft word and excel. Cryptology ePrint Archive, Report 2005/007, 2005.

[596] K. Wüst, K. Kostiainen, V. Capkun, and S. Capkun. Prcash: Fast, private and regulated transactions for digital currencies. In *Financial Cryptography*, 2018.

[597] Z. Xia and S. Schneider. A new receipt-free e-voting scheme based on blind signatures. In *WOTE*, 2006.

[598] Z. Xia, S. A. Schneider, and J. Heather. Analysis, improvement and simplification of pret a voter with paillier encryption. In *EVT*, 2008.

[599] N. Yang and J. Clark. Practical governmental voting with unconditional integrity and privacy. In *Financial Cryptography and Data Security*, 2017.

[600] A. C. Yao. Protocols for secure computations. In *IEEE FOCS*, 1982.

[601] Z. Ye, S. Smith, and D. Anthony. Trusted paths for browsers. *ACM TISSEC*, 8(2), 2005.

[602] P. F. Yeh. Using prediction markets to enhance us intelligence capabilities: A "standard & poors 500 index" for intelligence. *Studies in Intelligence*, 50(4), 2006.

[603] S. Yilek, E. Rescorla, H. Shacham, B. Enright, and S. Savage. When private keys are public: Results from the 2008 Debian OpenSSL vulnerability. In *IMC*, 2009.

[604] W. Yuen, P. Syverson, Z. Liu, and C. Thorpe. Intention-disguised algorithmic trading. In *Financial Cryptography*, 2010.

[605] F. Zagórski, R. Carback, D. Chaum, J. Clark, A. Essex, and P. L. Vora. Remotegrity: Design and use of an end-to-end verifiable remote voting system. In *ACNS*, 2013.

[606] B. Zhang and H.-S. Zhou. Statement voting. In *Financial Cryptography*, 2019.

[607] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi. Town crier: An authenticated data feed for smart contracts. In *ACM CCS*, CCS '16, pages 270–282, New York, NY, USA, 2016. ACM.

[608] L. Zhao, J. I. Choi, D. Demirag, K. R. B. Butler, M. Mannan, E. Ayday, and J. Clark. One-time programs made practical. In *Financial Cryptography*, 2019.

[609] M. Zusman. Leveraging the edge: abusing SSL VPNs. In *Black Hat USA*, 2008.

[610] M. Zusman. Criminal charges are not pursued: Hacking PKI. In *DEFCON 17*, 2009.

[611] M. Zusman and A. Sotirov. Sub-prime PKI: Attacking extended validation SSL. Technical report, Black Hat Security Briefings, 2009.